Data: 24/03/2025

Política de Segurança da Informação

POL.SI.01

Política do Sistema de Gestão do Grupo Galli

Sumário

Introdução 3
Sistemas Adquiridos 3
Gerenciamento de Mudanças 4
Acesso à Internet 4
Acesso Remoto 5
Acesso Físico 5
Antivírus 6
Direitos de Acesso e Senhas 7
Colaborador 8
Mesa Limpa 9
Tela Limpa 9
BYOD (Bring Your Own Device) 11
Utilização Profissional dos Recursos de TI 11
Regras de Utilização dos Recursos de TI 12
Política de Senhas 13
Utilização de Softwares 14
Rede WiFi 15
Demais Recursos de TI 16
Alimentos, Bebidas e Afins 17
Teletrabalho 18
Visitantes 19
Clientes 20
Auditoria e Monitoramento 21
Requisitos Legais e Normativos 21

1. Missão, Objetivos e Finalidade da Política

A presente Política de Segurança da Informação (PSI) do Grupo Galli tem como propósito estabelecer um conjunto robusto de orientações e controles que visam à proteção integral dos ativos de informação de todas as suas unidades e áreas de negócio. Reconhecendo a importância dos dados para a continuidade, a reputação e a conformidade legal do Grupo Galli, esta PSI aplica-se a todos os sócios, gestores, colaboradores, fornecedores e terceiros que tenham acesso a sistemas ou informações sob responsabilidade do Grupo Galli.

2. Papéis e Responsabilidades do Processo (MATRIZ RACI)

Legenda: (R) Responsável | (A) Aprovador | (C) Consultado | (I) Informado

Atividade	Cargo 1	Cargo 2	Cargo 3	Cargo 4
Desenvolvimento da Política	A	C	R	I
Implementação de Controles de Segurança	A	C	R	I
Treinamento e Conscientização	A	C	R	R
Monitoramento e Avaliação da Política	A	C	R	R
Respostas a incidentes de segurança	A	C	R	R

- Cargo 1: Diretoria
- Cargo 2: Financeiro
- Cargo 3: TI

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

3. Informação Documentada de Origem Interna e Externa Referenciadas

Informação Documentada de Origem Interna	Informação Documentada de Origem Externa
POL.QUA.01 - Política da Qualidade	ABNT NBR ISO IEC 27001 3ª ed. 23.11.2022
POL.SI.02 - Política de SI para Fornecedores	ABNT NBR ISO IEC 27701 1ª ed. 25.11.2019
POL.SI.03 - Política de Privacidade	ABNT NBR ISO 14001 3ª ed. 06.11.2015
PG.01 - Gestão Estratégica	ABNT NBR ISO 9001 3ª ed. 30.10.2015
PG.02 - Gestão de Riscos e Oportunidades	ABNT NBR ISO IEC 20000-1 3ª ed. 30.03.2020
PG.03 - Gestão da Comunicação Interna e Externa	ABNT NBR ISO 19011 3ª ed. 20.12.2018
PG.04 - Gestão da Informação Documentada	Lei n° 12.965/2014 - Marco Civil da Internet
PG.05 - Gestão de Auditorias Internas e Externas	Lei n° 12.737/2012 - Tipificação Criminal Informática
PG.06 - Gestão de Monitoramento, Medição e Análise	Lei no 13.709/2018 - Lei Geral de Proteção de Dados
PG.07 - Gestão de Não Conformidades e Ações Corretivas	Resolução CMN nº 4.893, de 26 de fevereiro de 2021
PG.08 - Gestão de RH	Decreto nº 11.856, de 26 de dezembro de 2023

4. Histórico de Revisões e Aprovações

Revisão	Data	Elaborador	Revisor	Aprovador	Descrição da Revisão
00	24/03/2025	Rafael Auwarter	Eduarda Kawasaki	Gabriel Galli	Emissão Inicial do Documento

5. Descrição das Diretrizes

5.1 Introdução

1. A segurança da informação é estratégica para o Grupo Galli, dadas as áreas sensíveis em que atua (serviços jurídicos, contábeis, financeiros, tributários e ambientais). Manter a confidencialidade, integridade e disponibilidade dos dados é essencial para garantir a satisfação dos clientes, o cumprimento de requisitos legais e a competitividade das unidades de negócio.

2. **Compromisso da Alta Administração:** A liderança do Grupo Galli reconhece a necessidade de investimentos contínuos em tecnologias, processos e pessoas que assegurem a robustez do Sistema de Gestão de Segurança da Informação (SGSI).

3. **Conscientização e Capacitação:** É dever de todos os integrantes (colaboradores, parceiros e terceiros autorizados) conhecer e aplicar as disposições desta PSI. O Grupo Galli realiza treinamentos, palestras e campanhas de sensibilização para difundir a cultura de segurança em todos os níveis.

4. **Revisão e Atualização**: A PSI deve acompanhar as evoluções tecnológicas e regulatórias, bem como as lições aprendidas em incidentes. As unidades podem encaminhar sugestões de melhoria à Equipe de Segurança da Informação, fortalecendo uma cultura de evolução constante.

5.2 Sistemas Adquiridos

1. **Avaliação de Segurança:** Todos os softwares, ferramentas e plataformas devem passar por testes de segurança e compliance antes de serem liberados para uso produtivo.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

2. **Avaliação de Segurança:** Antes de qualquer solução — seja ela um software, uma ferramenta ou uma plataforma de terceiros — ser introduzida no ambiente corporativo, é fundamental que ela seja submetida a testes de segurança. Esses testes podem incluir análises de vulnerabilidades, checagem de patches e revisões de configuração padrão, a fim de identificar possíveis pontos fracos que possam ser explorados.

3. **Conformidade Legal:** Desde a fase de análise da aquisição, devem-se mapear os requisitos legais e contratuais aplicáveis (leis, regulamentações do setor, acordos de confidencialidade etc.). Dessa forma, a organização garante que a solução final atenderá às obrigações de privacidade, proteção de dados e demais disposições vigentes. Alguns pontos de atenção:

    - Proteção de Dados e LGPD: Certificar-se de que o sistema adquirido cumpre normas de privacidade e preveja mecanismos para atender aos direitos dos titulares, conforme exigido pela Lei Geral de Proteção de Dados (LGPD) e outras regulamentações.
    - Cláusulas de confidencialidade: Acordos de não divulgação (NDA) devem proteger informações corporativas sensíveis, assegurando que nenhum dado da organização seja exposto indevidamente.

4. **Monitoramento Contínuo:** Após a implementação do sistema adquirido, é indispensável acompanhar de forma regular o seu desempenho e os eventos de segurança, para antecipar e mitigar incidentes.

5.3 Gerenciamento de Mudanças

1. **Foco no Cliente:** Cada unidade do Galli Group visa aprofundar o entendimento das necessidades do cliente, personalizando soluções e garantindo celeridade, precisão e confiabilidade na execução dos serviços.

2. **Processo Formalizado:** Solicitações de mudança são registradas, analisadas e aprovadas por instâncias competentes, evitando impactos indevidos.

3. **Avaliação de Impacto:** As equipes identificam potenciais riscos e planejam ações de mitigação antes de aprovar a mudança.

4. **Comunicação e Documentação:** Todos os envolvidos são informados das mudanças aprovadas, e a documentação do processo é mantida para auditorias e consultas.

5.4 Acesso à Internet

1. **Acesso:** No Grupo Galli, o acesso à Internet é gerenciado de forma a prevenir ameaças internas e externas que possam comprometer a confidencialidade, a integridade e a disponibilidade das informações.

2. **Controles de Acesso:** O Grupo Galli mantém firewalls atualizados com regras definidas para bloqueio e permissão (whitelists e blacklists) alinhadas às necessidades do negócio. Sistemas de detecção e prevenção de intrusão complementam a segurança, identificando e bloqueando invasões ou comportamentos maliciosos. Utilizamos soluções de filtragem de conteúdo para restringir o acesso a sites que apresentem risco de contaminação por malware, conteúdo ofensivo ou atividades ilícitas.

3. **Políticas de Uso Aceitável:** Todos os colaboradores do Grupo Galli tomam ciência de uma política formal que define usos permitidos e proibidos. A assinatura ou aceite digital confirma o entendimento e a adesão a essas regras. Autorizamos o uso pessoal da Internet em caráter limitado, desde que não interfira na produtividade, não acarrete riscos e siga as normas internas. Violações deliberadas ou graves das políticas de uso da Internet resultam em sanções disciplinares, conforme o regimento interno do Grupo Galli.

4. **Monitoramento do Tráfego:** Mantemos soluções para gestão, monitorando os históricos de navegação e identificando acessos suspeitos.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

5. **Educação dos Usuários:** Incentivamos todos os colaboradores a reportar incidentes, e-mails suspeitos ou quaisquer atividades anormais que possam indicar ameaças.

6. **Segurança em Nível de Rede:** Separamos logicamente as redes internas das redes para convidados (como Wi-Fi para visitantes), impedindo movimentações laterais de invasores. Aplicamos atualizações de firmware e correções de segurança em roteadores, switches e firewalls de forma contínua, evitando a exploração de vulnerabilidades conhecidas.

7. **Resposta a Incidentes:** Ao detectar acessos irregulares ou incidentes de segurança, o time responsável isola endpoints comprometidos, aciona o plano de resposta a incidentes e notifica as instâncias superiores.

8. **Registro e Aprendizado:** Cada incidente é documentado, analisado e transformado em lições aprendidas, possibilitando o aperfeiçoamento das defesas e a revisão de procedimentos.

5.5 Acesso Remoto

1. **Autenticação Forte:** O Galli Group, sempre que possível e aplicável, utiliza autenticação multifator (MFA) como padrão para acessos remotos a quaisquer sistemas críticos. Cada usuário autorizado deve adotar credenciais seguras (senhas complexas) e métodos adicionais de verificação (tokens, aplicativos de autenticação ou certificados digitais), de modo a reduzir substancialmente o risco de acessos indevidos.

2. **Uso de VPN Segura:** Quando aplicável, o acesso remoto às redes corporativas do Galli Group ocorre via Virtual Private Network (VPN), configurada com protocolos robustos de criptografia (por exemplo, TLS ou IPSec).

3. **Segregação de Ambientes:** Para preservar informações que exigem tratamento diferenciado – como documentos jurídicos da Galli Advogados, relatórios contábeis da Ivaí Gestão Financeira e dados estratégicos de Fiscalli, Ambientalli e Instituto Agroportuário –, o Galli Group opera redes virtuais ou ambientes separados que restringem o acesso apenas às equipes devidamente autorizadas. Essa segregação previne que usuários remotos, ainda que legítimos, tenham visibilidade além do necessário para suas funções.

4. **Monitoramento e Auditoria:** Qualquer anomalia, tentativa de invasão ou comportamento suspeito é prontamente investigado, e ações corretivas são tomadas em tempo hábil. Relatórios de auditoria são gerados periodicamente para comprovar conformidade com requisitos legais e normativos, reforçando a transparência e a confiabilidade do grupo.

5. **Atualização e Manutenção de Segurança:** As soluções de VPN, firewalls e demais ferramentas utilizadas no acesso remoto passam por revisões técnicas e pela aplicação de correções (patches) de segurança assim que são disponibilizadas pelos respectivos fornecedores.

6. **Resposta a Incidentes:** Em caso de suspeita ou confirmação de acesso indevido, o Galli Group aciona seu plano de resposta a incidentes, isolando rapidamente o ponto de entrada e implementando ações que protejam a confidencialidade e a integridade das informações afetadas. Esse procedimento segue diretrizes específicas, contemplando a contenção do incidente, a restauração do ambiente seguro e a notificação de partes interessadas quando necessário.

7. **Política de Dispositivos Remotos:** Qualquer equipamento que seja utilizado para acessar remotamente as redes e sistemas do Galli Group deve cumprir os requisitos mínimos de segurança estabelecidos na PSI, incluindo antivírus atualizado e configurações de firewall ativas. Assim, assegura-se que o ponto final (endpoint) não se torne vetor de ameaças para a infraestrutura corporativa.

5.6 Acesso Físico

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

1. **Controle de Acesso Físico:** O Galli Group determina que apenas pessoas expressamente autorizadas possam ingressar em locais críticos e áreas de armazenamento de dados, como salas de servidores, arquivos confidenciais e depósitos de documentos estratégicos. Essa autorização prévia, registrada em sistemas específicos ou em livros de controle, assegura que as instalações permaneçam restritas e protegidas contra acessos não aprovados.

2. **Autenticação e Registro:** Para manter a rastreabilidade, qualquer entrada em áreas seguras do Galli Group é condicionada a procedimentos de identificação, como a verificação de crachás, senhas ou biometria. Visitantes externos, fornecedores e prestadores de serviço devem ser registrados em um sistema de controle que registre nome, data, horário de entrada e saída, bem como a motivação da visita. Esse cuidado é fundamental para salvaguardar os dados relacionados às atividades das unidades Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário.

3. **Medidas de Segurança Física:** Em cada unidade do Galli Group, são adotados dispositivos e mecanismos de segurança, tais como:

    - Câmeras de Vigilância (CFTV) que monitoram 24 horas por dia corredores, salas e demais pontos de acesso.
    - Alarmes e Sensores de presença ou de movimento, que detectam tentativas de invasão ou movimentações fora do horário padrão.
    - Portas e Barreiras Físicas reforçadas com fechaduras de segurança e mecanismos de travamento.

4. **Segregação de Ambientes Críticos:** Reconhecendo que cada unidade do Galli Group lida com dados específicos (advocatícios, tributários, ambientais, financeiros etc.), a segregação de ambientes críticos é praticada de forma rigorosa. Isso evita o contato indevido entre diferentes bases de dados e serviços, promovendo a segurança e o isolamento de informações estratégicas.

5. **Gestão de Equipamentos e Infraestrutura:** Documentos físicos devem ser guardados em armários ou arquivos trancados, com acesso limitado às equipes responsáveis. Prestadores de serviços de manutenção (elétrica, climatização, rede física) só podem acessar áreas restritas do Galli Group após validação e acompanhamento de um profissional interno. Onde aplicável, há sistemas de proteção contra incêndio, controle de temperatura e umidade, garantindo a preservação de documentos e equipamentos críticos que abrigam informações do Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário.

6. **Acompanhamento de Visitantes e Terceiros:** Sempre que visitantes ou terceiros necessitam entrar em áreas sensíveis das instalações do Galli Group, eles são acompanhados por um profissional autorizado, que permanece responsável pelo monitoramento das atividades durante o período de permanência do visitante. Este processo evita o acesso, manuseio ou visualização não autorizada de dados, protegendo especialmente os acervos ligados aos serviços de consultoria jurídica, tributária, ambiental e de gestão financeira.

7. **Registro e Auditoria:** O Galli Group mantém histórico de todos os acessos físicos ocorridos nas dependências de cada unidade, incluindo registros de data, hora, nome do visitante ou colaborador, motivo do acesso e local visitado. Com base nesse histórico, o time de Segurança da Informação realiza verificações periódicas para confirmar que todos os acessos foram conduzidos em conformidade com as normas e que não há indícios de comportamentos irregulares.

8. **Incidentes de Segurança Física:** Qualquer incidente ou tentativa de violação no acesso físico é reportado imediatamente à equipe de Segurança do Galli Group. Ao identificar falhas ou vulnerabilidades, a organização adota ações corretivas e preventivas para evitar recorrências, mantendo a excelência e a segurança de suas operações.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

5.7 Antivírus

1. **Cobertura Obrigatória:** Todas as estações de trabalho, servidores e dispositivos conectados à rede do Galli Group devem ter, obrigatoriamente, um software antivírus devidamente instalado e configurado. Esse requisito estende-se às unidades Galli Advogados, Fiscalli, Ambientalli, Ivaí Gestão Financeira e Instituto Agroportuário, independentemente da finalidade do equipamento ou do setor de atuação.

2. **Atualizações e Assinaturas:** O Galli Group assegura que as definições de vírus e as versões de software antivírus sejam atualizadas de forma automática, diária ou em ciclos pré-definidos, de acordo com as recomendações do fornecedor. Assim, prevenimos que vulnerabilidades conhecidas afetem os serviços jurídicos, contábeis, financeiros, tributários e ambientais prestados por cada unidade.

3. **Verificações Periódicas:** Implementamos rotinas de varredura (scans) para detecção de malwares em intervalos regulares e definimos mecanismos de análise de logs que reportam eventuais anomalias para a equipe responsável pela segurança da informação do Galli Group. Dessa forma, as unidades atuam preventivamente na identificação e contenção de ameaças.

4. **Isolamento e Tratamento de Incidentes:** Em caso de detecção de arquivos maliciosos ou comportamentos suspeitos, o Galli Group adota procedimentos de isolamento imediato do dispositivo. Em seguida, conduz-se um processo de análise e desinfecção rigoroso, garantindo que as informações manuseadas nas áreas jurídica, contábil, financeira, tributária e ambiental permaneçam intactas e seguras.

5. **Integração com o SGSI:** O antivírus não atua de forma isolada; ele integra-se aos demais controles previstos no SGSI do Galli Group, complementando as camadas de proteção que asseguram a confidencialidade, a integridade e a disponibilidade das informações estratégicas.

6. **Conscientização de Usuários:** Além das medidas tecnológicas, o Galli Group enfatiza a conscientização dos colaboradores de cada unidade, instruindo-os sobre o papel crucial que o antivírus desempenha na prevenção de infecções e alertando sobre práticas de risco, como a abertura de e-mails suspeitos ou o uso de dispositivos de armazenamento sem procedência confiável.

5.8 Direitos de Acesso e Senhas

1. **Princípio do Menor Privilégio:** O Galli Group promove o fornecimento de direitos de acesso somente na medida exata do que é necessário para a realização das atividades de cada pessoa ou equipe. Esse procedimento evita que colaboradores ou terceiros tenham acesso a informações que não sejam pertinentes a suas funções, assegurando a confidencialidade dos dados.

2. **Matriz de Acesso e Revisão Periódica:** Cada unidade do Galli Group mantém uma matriz de acesso detalhada, definindo quais perfis e cargos podem visualizar, criar, modificar ou excluir informações. Essa matriz é revisada periodicamente para verificar a adequação dos privilégios concedidos. Em situações de mudança de função, promoção ou desligamento, as autorizações são imediatamente atualizadas, reduzindo riscos de acessos indevidos.

3. **Criação de Senhas e Práticas Seguras:** As contas de usuários dentro do escopo do SGSI do Galli Group devem obedecer à política de senhas robustas, contemplando tamanhos mínimos, uso de caracteres especiais, alternância entre maiúsculas e minúsculas e renovação periódica. Fica expressamente proibido anotar senhas em locais de fácil acesso ou compartilhá-las com terceiros. A organização realiza campanhas de conscientização destacando a importância de não utilizar senhas simples ou repetidas em diferentes plataformas, reforçando a postura proativa de segurança na rotina dos colaboradores.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

4. **Autenticação Multifator (MFA):** Para sistemas e aplicações considerados críticos – em especial aqueles que lidam com dados jurídicos, tributários e financeiros das unidades do Galli Group – é adotado o uso obrigatório de autenticação multifator (MFA). Dessa forma, mesmo que ocorra comprometimento de uma senha, a segunda camada de autenticação dificulta ações mal-intencionadas e protege a integridade das informações.

5. **Controle de Sessões e Bloqueio de Contas:** As contas de usuário são submetidas a bloqueio automático após um número pré-definido de tentativas de login sem sucesso, prevenindo ataques de força bruta. Além disso, períodos de inatividade superiores a determinados limites promovem o bloqueio ou o encerramento automático de sessão, impedindo que um terminal logado seja acessado por terceiros sem autorização.

6. **Revogação Imediata de Acessos:** Sempre que um colaborador, fornecedor ou parceiro do Galli Group se desliga do projeto ou encerra seu vínculo com a empresa, seu acesso é imediatamente revogado. A política prevê processos documentados de retirada de privilégios, bem como a comunicação aos responsáveis pela área de TI, minimizando o risco de acessos não autorizados e assegurando a conformidade com o SGSI.

7. **Responsabilidade e Rastreamento:** Cada usuário é responsável pelas ações realizadas com suas credenciais. As atividades de acesso aos sistemas corporativos são registradas em logs, permitindo que o Galli Group faça a rastreabilidade de eventos de segurança e identifique incidentes ou comportamentos suspeitos. As revisões desses registros são conduzidas de forma sistemática, a fim de detectar quaisquer inconsistências ou acessos fora do padrão, fortalecendo a postura preventiva contra vazamentos e ameaças internas.

8. **Apoio na Resolução de Incidentes:** Em caso de suspeita de acesso indevido ou comprometimento de contas de usuário, o Galli Group aciona imediatamente os procedimentos de resposta a incidentes, incluindo a redefinição de senhas, o bloqueio temporário de contas e a abertura de investigação formal. Esse processo é executado de maneira ágil e eficaz, alinhado às melhores práticas e às normas internas de segurança.

5.9 Colaborador

1. **Responsabilidade Individual e Compromisso com a Segurança:** Cada colaborador do Galli Group deve conduzir suas atividades de forma diligente, seguindo as diretrizes estabelecidas neste Sistema de Gestão da Segurança da Informação (SGSI). É imperativo reportar de imediato qualquer incidente, suspeita de violação ou situação que coloque em risco os ativos informacionais do Galli Group. A omissão ou a negligência no reporte de problemas podem prejudicar não apenas a organização, mas também os clientes que confiam na solidez de nossas operações.

2. **Adesão às Políticas e Procedimentos:** O cumprimento irrestrito das políticas internas – incluindo regras de senha, acesso físico e virtual, uso de dispositivos pessoais (BYOD) e classificação de documentos – é obrigatório. Violações intencionais ou descaso na aplicação dessas diretrizes não serão toleradas, pois colocam em risco a segurança das informações processadas pelo Galli Group nas mais diversas frentes de negócio.

3. **Proteção de Informações Confidenciais e Estratégicas:** Em um ambiente que lida com dados altamente sigilosos e regulados, seja na esfera jurídica, contábil, financeira, tributária ou ambiental, a confidencialidade deve ser preservada em todos os níveis. É proibido divulgar ou compartilhar dados sensíveis sem autorização prévia e formal. A cultura de segurança do Galli Group exige que cada colaborador zele pela integridade das informações sob sua responsabilidade e se conscientize sobre a importância de não expor qualquer dado que possa comprometer a reputação ou a legalidade das operações.

4. **Engajamento em Treinamentos e Capacitações:** O Galli Group promove treinamentos, workshops e reciclagens periódicas para garantir que todos estejam atualizados sobre as melhores práticas de segurança, novas ameaças e mudanças regulatórias que impactem o SGSI. A participação ativa nessas iniciativas reflete o compromisso

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

individual de cada colaborador em manter o Galli Group alinhado às normas vigentes e aos mais altos padrões de proteção de dados.

5. **Consequências e Sanções:** Qualquer atitude que provoque ou facilite vazamento, destruição, alteração indevida ou uso não autorizado de informações estratégicas será avaliada sob a ótica das políticas internas do Galli Group e, se necessário, poderá acarretar medidas disciplinares, sanções legais ou rescisão de contrato. Esse rigor visa proteger não apenas o interesse do Galli Group, mas também o das partes interessadas que depositam sua confiança nos serviços ofertados.

5.10 Mesa Limpa

1. **Obrigatoriedade de Organização Física:** O Galli Group estabelece que cada colaborador ou prestador de serviço mantenha sua estação de trabalho livre de documentos físicos quando estes não estiverem em uso imediato. Pastas, relatórios, contratos e quaisquer impressos devem ser guardados em gavetas ou armários fechados, para impedir a visualização ou o manuseio não autorizado.

2. **Armazenamento Seguro de Documentos:** Qualquer informação confidencial, seja um contrato de consultoria tributária, um processo jurídico ou registros financeiros, deve ser armazenada em locais adequados, como cofres, armários com chave ou áreas de arquivo designadas pelo Galli Group. O acesso a esses locais é restrito de acordo com as responsabilidades e o nível de confidencialidade dos dados.

3. **Responsabilidade Individual:** Cada profissional das unidades do Galli Group é afirmativamente responsável por proteger os dados sob sua custódia. Ao se ausentar do posto de trabalho, o colaborador deve guardar qualquer documento sensível em local trancado e remover da mesa itens que possam expor informações relevantes do cliente ou do próprio Galli Group.

4. **Digitalização e Descarte de Documentos:** O Galli Group incentiva a digitalização de arquivos físicos, observando procedimentos seguros de conversão e armazenamento digital. Quando documentos impressos se tornam obsoletos ou desnecessários, devem ser fragmentados ou descartados de maneira segura, evitando risco de recuperação indevida.

5. **Inspeções e Auditorias Internas:** Equipes de segurança e gestores têm permissão e autoridade para realizar inspeções periódicas, verificando a aderência dos colaboradores à política de Mesa Limpa. Em caso de inconformidades, ações corretivas são adotadas para reforçar a cultura de segurança da informação, sempre preservando o propósito de proteger os dados estratégicos do Galli Group.

6. **Interface com o Teletrabalho:** Profissionais em regime remoto também devem praticar a Mesa Limpa em seu ambiente domiciliar ou em espaços de coworking. Isso inclui manter pastas e impressões em locais seguros, livres de acesso por terceiros. O Galli Group afirma a responsabilidade de cada colaborador por zelar pela proteção dos documentos mesmo fora das instalações físicas oficiais.

7. **Benefícios e Impacto Positivo:**

   - Redução de Riscos: Diminui consideravelmente o risco de vazamentos, roubos ou furtos de documentos sensíveis e estratégicos do Galli Group.
   - Ambiente Profissional: Uma mesa organizada e limpa demonstra comprometimento com padrões de segurança e eleva a imagem profissional das unidades do grupo.
   - Eficiência e Agilidade: Favorece a localização rápida de documentos e equipamentos, evitando atrasos em rotinas jurídicas, contábeis, financeiras, tributárias e ambientais.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

8. **Penalidades e Consequências do Não Cumprimento:** O descumprimento desta política é avaliado conforme o Código de Ética e Conduta do Galli Group. A não observância repetida ou proposital destas diretrizes resulta em sanções disciplinares, que podem variar de advertências a medidas mais graves, dependendo da gravidade e recorrência da infração.

5.11 Tela Limpa

1. **Objetivo do Requisito:** Evitar a visualização não autorizada de informações: A medida de Tela Limpa garante que dados confidenciais ou estratégicos não sejam vistos por terceiros que transitam ou compartilham o mesmo ambiente de trabalho. Reforçar a cultura de segurança no Galli Group: Ao implementar práticas de Tela Limpa, fomentamos o senso de responsabilidade individual e coletiva, pois todos passam a adotar comportamentos que preservem o sigilo das operações em andamento.

2. **Aplicabilidade e Abrangência:** Aplica-se a todas as unidades do Galli Group (Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário), abrangendo colaboradores, estagiários, terceirizados e quaisquer outros profissionais que utilizem sistemas e terminais de acesso corporativos. Deve ser observada em todos os ambientes onde informações sensíveis ou estratégicas sejam manuseadas, incluindo salas de atendimento, estações de trabalho, áreas de coworking e instalações de clientes ou parceiros, quando houver acesso remoto às bases de dados do Galli Group.

3. **Regras e Práticas de Implementação**

- Bloqueio automático de tela: As estações de trabalho e dispositivos eletrônicos devem ser configurados para bloquear a tela automaticamente após período pré-definido de inatividade. O tempo padrão de inatividade será definido pelas equipes de segurança e TI, balanceando produtividade e proteção de dados.
- Bloqueio manual ao se ausentar: Sempre que um usuário do Galli Group se afastar de sua estação de trabalho (mesmo que temporariamente), deve acionar manualmente o bloqueio de tela ou o modo “sleep” protegido por senha.
- Confidencialidade de documentos abertos: Em atividades que envolvam exibição de documentos jurídicos, planilhas financeiras, análises tributárias ou relatórios ambientais, recomenda-se minimizar ou encerrar a exibição desses arquivos antes de receber visitantes, atender telefonemas ou envolver-se em qualquer tarefa que possa distrair a atenção da tela.
- Uso de protetores de tela ou filtros de privacidade: Em ambientes de maior risco (salas de espera, espaços abertos ou áreas compartilhadas), pode-se recorrer a protetores físicos que dificultem a leitura lateral da tela, reduzindo a exposição de dados confidenciais aos que circulam no local.
- Formação e orientação contínua: Treinamentos internos do Galli Group reforçam periodicamente a importância dessa prática, descrevendo cenários de risco e exemplificando como pequenos descuidos podem gerar grandes prejuízos à organização e aos clientes.

4. **Benefícios para a Segurança das Informações**

- Proteção contra acesso casual ou oportunista: O bloqueio de tela impede que pessoas não autorizadas tenham contato com dados de alto valor (financeiros, jurídicos, tributários, ambientais etc.).
- Prevenção de incidentes: Minimiza a probabilidade de vazamentos e incidentes internos, reforçando o controle de quem pode visualizar informações críticas do Galli Group.
- Demonstração de conformidade: Facilita o cumprimento de requisitos de normas como a ISO/IEC 27001 e regulamentos correlatos (LGPD, legislações setoriais), evidenciando boa governança e proteção de dados sensíveis.
- Fortalecimento da cultura de segurança: Ao abraçar práticas de Tela Limpa, cada colaborador percebe seu papel vital na manutenção do SGSI (Sistema de Gestão da Segurança da Informação), tornando-se agente ativo de preservação do sigilo profissional.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

5. Responsabilidades e Sanções

- Responsabilidade do Usuário: Cada colaborador do Galli Group é diretamente responsável por bloquear a tela quando se ausenta ou finaliza tarefas, sobretudo ao lidar com dados em áreas comuns ou propensas a movimentação de pessoas.
- Monitoramento e Revisão: A equipe de Segurança da Informação realiza verificações pontuais e auditorias para constatar a aderência à política de Tela Limpa, podendo recomendar ajustes ou melhorias no processo.
- Sanções por descumprimento: O descumprimento das regras de Tela Limpa pode acarretar medidas disciplinares, variando desde advertências até o desligamento, caso se comprove que a omissão resultou em incidente grave ou dano significativo à privacidade e à reputação do Galli Group e de seus clientes.

5.12 BYOD (Bring Your Own Device)

1. **Objetivo do Requisito:** Estabelecer diretrizes para o uso de dispositivos pessoais no ambiente corporativo, garantindo a proteção dos dados e a segurança da rede. Visa assegurar que os dispositivos atendam aos padrões de segurança necessários, minimizando riscos de vazamento de informações e acessos não autorizados. A política busca equilibrar a flexibilidade com a conformidade às normas de segurança da organização.

2. **Requisitos de Conformidade:** Todos os colaboradores e parceiros do Galli Group que desejarem utilizar dispositivos pessoais (laptops, tablets, smartphones ou outros) devem garantir que esses equipamentos atendam aos critérios mínimos de segurança definidos pela área de TI do Galli Group, incluindo sistemas operacionais atualizados, antivírus ativo e uso de senhas fortes. Assim, assegura-se a proteção das informações sensíveis e estratégicas processadas ou armazenadas.

3. **Restrições e Acesso:** O Galli Group exige que o acesso a informações críticas ou que envolvam dados de clientes e parceiros seja feito mediante autenticação robusta (por exemplo, MFA – Multi-Factor Authentication). Dessa forma, asseguramos a confidencialidade, integridade e disponibilidade dos dados relativos aos serviços das áreas jurídica, contábil, financeira, tributária e ambiental, reduzindo o risco de acessos não autorizados.

4. **Gestão e Monitoramento:** A equipe de TI do Galli Group pode executar varreduras e auditorias para verificar a conformidade dos dispositivos com as políticas internas de segurança. Isso inclui, entre outros pontos, análise de aplicativos instalados, versões de softwares, atualizações de segurança e evidências de possíveis vulnerabilidades que possam colocar em risco os dados corporativos. Constatada qualquer violação às diretrizes do SGSI, o Galli Group realizará medidas imediatas para isolar o dispositivo infrator, prevenindo a propagação de ameaças ou o vazamento de informações.

5. **Políticas de Privacidade e Proteção de Dados:** O Galli Group reitera a obrigatoriedade de respeitar a privacidade dos colaboradores no uso de seus dispositivos pessoais, mas enfatiza que a segurança dos dados de clientes, parceiros e do próprio Grupo tem precedência. Qualquer verificação ou intervenção técnica no dispositivo pessoal será efetuada em conformidade com as leis vigentes e as políticas de privacidade adotadas pelo Galli Group.

6. **Responsabilidade e Termo de Compromisso:** Todos os usuários que aderirem à política de BYOD devem assinar um termo de compromisso, declarando-se cientes das regras de segurança e assumindo a responsabilidade pelo manuseio de informações e dados corporativos. Em caso de perda ou roubo de dispositivo, o Galli Group deve ser informado imediatamente para possibilitar a adoção de medidas de contenção (bloqueio remoto, revogação de certificados, alteração de credenciais etc.).

7. **Remoção de Dados e Término do Vínculo:** Se um colaborador ou parceiro deixar de prestar serviços ao Galli Group, ou mudar para uma função que não requeira BYOD, a TI realizará a exclusão segura de quaisquer informações

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

corporativas mantidas no dispositivo. Isso assegura que os dados confidenciais relacionados aos serviços das unidades sejam removidos, minimizando a possibilidade de vazamentos ou utilizações indevidas pós-desligamento.

5.13 Utilização Profissional dos Recursos de TI

1. **Uso Exclusivamente Profissional:** O Grupo Galli determina que computadores, dispositivos móveis, softwares, plataformas de colaboração, impressoras, redes de comunicação, entre outros recursos tecnológicos, sejam utilizados apenas para finalidades de trabalho. Todo colaborador é afirmativamente responsável por assegurar que suas atividades contribuem para a eficiência operacional e para a proteção dos dados sensíveis do Grupo Galli e de seus clientes.

2. **Aderência às Políticas de Segurança:** Cada usuário deve cumprir rigorosamente as políticas de segurança estabelecidas pelo SGSI do Grupo Galli. Isso inclui manter configurações adequadas de seus equipamentos, atualizar periodicamente sistemas e aplicativos, não instalar softwares não autorizados e observar as diretrizes de confidencialidade, integridade e disponibilidade dos dados. A violação destes princípios pode comprometer diretamente os serviços jurídicos, contábeis, financeiros, tributários ou ambientais prestados pelas unidades.

3. **Monitoramento e Auditoria:** O Grupo Galli se reserva o direito de monitorar e auditar o uso profissional dos recursos de TI para salvaguardar informações estratégicas e sensíveis. Essa medida é necessária para detectar possíveis abusos, incidentes de segurança e situações de não conformidade com a Política de Segurança da Informação, assegurando que as operações do Grupo Galli se mantenham dentro dos padrões esperados.

4. **Responsabilidade Pessoal e Coletiva:** Ao utilizar os recursos de TI, o colaborador assume a responsabilidade de proteger não apenas a si mesmo, mas também o Grupo Galli como um todo. A manipulação negligente de dados, o compartilhamento não autorizado de informações, a execução de tarefas alheias ao trabalho ou a prática de atos ilícitos colocam em risco tanto o colaborador quanto a reputação e a perenidade dos negócios do Grupo Galli.

5. **Prevenção de Ameaças e Não Conformidades:** Por lidar com dados altamente confidenciais, seja na esfera jurídica, tributária, financeira, contábil ou ambiental, o Grupo Galli exige que os colaboradores atentem para quaisquer potenciais ameaças que surjam no cotidiano de trabalho – por exemplo, mensagens de phishing, links suspeitos, anexos duvidosos ou downloads não autorizados. Toda e qualquer suspeita deve ser imediatamente reportada à Equipe de Segurança da Informação para análise e tratamento, reforçando o espírito colaborativo no cuidado com os ativos informacionais.

6. **Uso Racional de Recursos:** O Grupo Galli incentiva o uso racional e sustentável dos recursos de TI, respeitando a política de consumo consciente, evitando desperdício de papel, tinta e energia elétrica. Uma gestão adequada de recursos reflete diretamente no compromisso com a responsabilidade socioambiental e na imagem da organização perante clientes e stakeholders.

7. **Aplicação de Medidas Disciplinares:** Em caso de descumprimento reiterado ou grave das diretrizes de utilização profissional dos recursos de TI, o colaborador estará sujeito a medidas disciplinares, de acordo com o código interno do Grupo Galli e a legislação vigente. A integridade do ambiente de TI é fundamental para que o SGSI seja efetivo e para que os serviços prestados em cada unidade mantenham-se ininterruptos e em conformidade com os requisitos normativos.

5.14 Regras de Utilização dos Recursos de TI

1. **Definição e Abrangência:** As Regras de Utilização dos Recursos de TI do Grupo Galli englobam todos os meios tecnológicos fornecidos pela organização, incluindo computadores, notebooks, dispositivos móveis, redes, sistemas em nuvem, acesso à Internet, plataformas de software e demais ferramentas que tratem ou transportem informações relacionadas aos nossos serviços multidisciplinares. O objetivo é garantir que o uso desses recursos

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

seja sempre coerente com a finalidade de negócio de cada unidade, evitando riscos que possam comprometer a segurança dos dados.

2. Uso Permitido e Restrições

- Finalidade Corporativa: O uso dos recursos de TI deve sempre priorizar as atividades profissionais e estar alinhado ao suporte legal, contábil, financeiro, tributário ou ambiental prestado pelas unidades do Grupo Galli.
- Restrições: É expressamente proibida a instalação e execução de softwares não autorizados, o acesso a sites maliciosos ou ilegais e qualquer outra prática que possa violar leis, regulamentos ou práticas éticas de mercado.
- Zelo e Proteção: Todos os usuários devem zelar pela proteção de dados sensíveis, abstendo-se de armazenar documentos críticos em locais não seguros ou compartilhar credenciais de acesso.

3. Responsabilidade do Usuário: Cada profissional vinculado ao Grupo Galli é responsável pelo uso correto dos recursos de TI que lhe são disponibilizados. O desvio intencional ou negligente dessas normas pode acarretar consequências que vão desde medidas disciplinares internas até repercussões legais, dependendo do grau de infração e do potencial impacto negativo para a organização ou para clientes.

4. Monitoramento e Conformidade

- Acompanhamento das Atividades: O Grupo Galli reserva-se o direito de monitorar o uso de recursos de TI, sempre em conformidade com a legislação aplicável e as políticas internas de privacidade e segurança. Esse acompanhamento tem como finalidade identificar atividades suspeitas, prevenir incidentes e, caso necessário, intervir para minimizar danos ao ambiente corporativo.
- Relatório de Irregularidades: Qualquer prática em desacordo com esta Política deve ser reportada imediatamente à equipe de Segurança da Informação ou ao gestor responsável, para que sejam adotadas as medidas corretivas cabíveis.

5. Proteção da Confidencialidade, Integridade e Disponibilidade: Ao cumprir integralmente as Regras de Utilização dos Recursos de TI, o Grupo Galli assegura a robustez do seu SGSI, permitindo o devido controle sobre dados estratégicos em todas as unidades. Assim, as informações jurídicas, contábeis, financeiras, tributárias e ambientais permanecem devidamente protegidas contra ameaças internas e externas, reforçando a confiança depositada pelos nossos clientes e parceiros.

5.15 Política de Senhas

1. Criação de Senhas Fortes

- Composição Complexa: As senhas devem conter sempre que possível, no mínimo, oito caracteres e devem incluir letras maiúsculas e minúsculas, números e caracteres especiais (por exemplo, @, #, %). Essa prática visa tornar mais difícil a descoberta por meio de ataques de força bruta ou de dicionário.
- Proibição de Sequências Óbvias: Sequências numéricas (como “1234”) ou letras em ordem alfabética não podem integrar as senhas, pois tais combinações facilitam a ação de invasores.
- Informações Pessoais: Qualquer dado pessoal (nome, data de nascimento, CPF, entre outros) não deve ser utilizado na senha, evitando associações que possam ser adivinhadas por terceiros mal-intencionados.

2. Confidencialidade e Responsabilidade

- Sigilo de Credenciais: Cada colaborador, gestor ou terceiro autorizado no Galli Group é o único responsável pela proteção de sua senha. O compartilhamento de credenciais é terminantemente proibido, independentemente do grau de confiança existente entre usuários.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

- Armazenamento Seguro: É inaceitável anotar senhas em papéis, planilhas ou locais desprotegidos. Recomenda-se o uso de gerenciadores de senhas confiáveis, que empreguem criptografia robusta, para arquivar credenciais com segurança.
- Responsabilização por Uso Indevido: Caso haja qualquer atividade executada em um sistema por meio de credenciais associadas a um determinado usuário, este poderá ser responsabilizado pela ação, reforçando a necessidade de rigorosos cuidados no manuseio das senhas.

3. Alteração e Ciclo de Vida das Senhas

- Validade Programada: Sempre que possível, o Galli Group estabelece prazos para expiração de senhas críticas. A troca periódica reduz o risco de um terceiro manter acesso indevido por tempo prolongado.
- Renovação Imediata por Suspeita de Violação: Ao menor indício de comprometimento de senha, o usuário deve alterá-la imediatamente e reportar o incidente ao setor de Segurança da Informação.
- Lembrança de Senhas: Sistemas que exijam troca regular podem alertar os colaboradores quando se aproxima o prazo de expiração, incentivando a renovação antecipada.

4. Múltiplos Fatores de Autenticação (MFA)

- Requisito para Acessos Críticos: Para áreas de maior sensibilidade, como contas com privilégios administrativos ou acesso a dados estratégicos (p. ex., informações tributárias da Fiscalli, documentos jurídicos da Galli Advogados ou relatórios financeiros da Ivaí Gestão Financeira), é obrigatório utilizar métodos de MFA (código enviado ao celular, token físico, aplicativos específicos, etc.).
- Redução de Riscos: O MFA torna o acesso indevido mais difícil, mesmo em casos de violação ou descoberta da senha principal. Assim, a confidencialidade e a integridade das informações permanecem asseguradas.

5. Senhas em Serviços em Nuvem e Aplicativos Terceirizados

- Verificação de Conformidade: Ao contratar soluções ou plataformas externas, o Galli Group verifica se os provedores oferecem mecanismos de autenticação segura e aderentes às políticas de senhas aqui descritas.
- Isolamento de Credenciais: Cada usuário deve ter uma conta pessoal, impedindo o uso de senhas genéricas ou compartilhadas, especialmente na execução de serviços ambientais (Ambientalli) ou em projetos de consultoria tributária (Fiscalli).
- Integração com Autenticação Corporativa: Quando possível, soluções em nuvem são integradas ao método corporativo de autenticação, centralizando o controle de senhas e facilitando auditorias.

5.16 Utilização de Softwares

1. **Software Autorizado:** O Galli Group determina que somente softwares previamente avaliados e aprovados possam ser instalados em estações de trabalho, servidores ou dispositivos utilizados em qualquer unidade do Grupo (Galli Advogados, Fiscalli, Ambientalli, Ivaí, Instituto Agroportuário). Essa medida assegura que aplicações maliciosas ou potencialmente inseguras não coloquem em risco os dados confidenciais relacionados aos serviços jurídicos, contábeis, financeiros, tributários e ambientais. Antes da implementação de um software em ambiente produtivo, realiza-se uma análise de vulnerabilidades e riscos alinhada aos objetivos do SGSI do Galli Group, garantindo que a ferramenta não represente ameaças à estabilidade ou à segurança das informações.

2. **Licenciamento e Conformidade:** Cada licença de software deve estar devidamente regularizada, observando leis de propriedade intelectual e acordos de uso. O Galli Group repudia expressamente o uso de softwares pirateados ou sem o devido registro, pois, além de infringir dispositivos legais, tais práticas abrem brechas de segurança que podem comprometer a integridade dos dados sensíveis das unidades Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário. A equipe de TI ou o setor responsável pela Gestão de Licenças monitora de modo contínuo o inventário de softwares para manter a conformidade com normas nacionais, internacionais e com as exigências do SGSI do Galli Group.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

3. **Atualizações e Patches de Segurança:** Em consonância com o compromisso do Galli Group de proteger ativos informacionais, todos os softwares instalados devem ser mantidos atualizados, seguindo as melhores práticas do mercado e os lançamentos de correções (patches) fornecidos pelos fabricantes. Essa abordagem preventiva reduz riscos de vulnerabilidades exploráveis, preservando a confidencialidade e a disponibilidade de dados estratégicos. Os setores e unidades que compõem o Galli Group são igualmente responsáveis por sinalizar eventuais atrasos nas atualizações ou quaisquer problemas relacionados, permitindo que a equipe de TI ou o Comitê de Segurança atue rapidamente.

4. **Auditoria e Inventário de Software:** Periodicamente, o Galli Group realiza auditorias internas para verificar a conformidade dos softwares instalados, cruzando os resultados com o inventário de licenças. Quaisquer aplicativos não autorizados ou desatualizados são identificados e removidos ou regularizados conforme os protocolos de segurança e de governança do Galli Group. Durante as auditorias, o time de Segurança da Informação avalia também o alinhamento dos aplicativos às necessidades operacionais de cada unidade (Galli Advogados, Fiscalli, Ambientalli, Ivaí, Instituto Agroportuário), de modo a garantir eficiência e redução de riscos na execução das atividades jurídicas, contábeis, financeiras, tributárias e ambientais.

5. **Remoção de Software Não Autorizado:** Caso seja detectada a presença de software não autorizado em qualquer dispositivo do Galli Group, o responsável pelo equipamento será notificado imediatamente para a correção da situação. A remoção é executada sem exceções, a fim de salvaguardar as informações sensíveis e estratégicas processadas no SGSI do Galli Group. Em casos de reincidência ou violação grave, aplicam-se medidas disciplinares que podem variar de advertências formais até desligamentos ou ações legais, dependendo do impacto e da exposição dos dados do Galli Group.

6. **Responsabilidade e Consciência de Riscos:** Todos os usuários, sejam colaboradores diretos ou terceiros autorizados, devem estar conscientes de que a instalação e o uso de softwares sem autorização colocam em risco a confidencialidade de informações jurídicas, contábeis, financeiras, tributárias e ambientais que circulam dentro do Galli Group. A manutenção da disponibilidade dos serviços nas áreas de atuação é diretamente vinculada ao uso correto e seguro dos aplicativos, reforçando a necessidade de um comportamento ético e aderente à presente política.

7. **Integração com Processos Críticos:** Em situações em que um software seja fundamental para rotinas específicas, como a análise de dados tributários (Fiscalli), a gestão de processos jurídicos (Galli Advogados), a condução de estudos ambientais (Ambientalli) ou a organização de fluxos financeiros (Ivaí), deverão ser estabelecidos critérios técnicos claros que confirmem a aderência da solução à PSI e ao SGSI do Galli Group. Qualquer modificação, substituição ou desativação de tais softwares deve passar pelo processo de Gerenciamento de Mudanças (Change Management), com avaliação multidisciplinar e testes de segurança para evitar prejuízos à integridade dos dados ou interrupções de serviço.

8. **Alinhamento à Visão Estratégica do Galli Group:** A Política de Utilização de Softwares faz parte da visão mais ampla de segurança e governança do Galli Group, respaldada por normativas e leis como LGPD, Marco Civil da Internet e padrões internacionais (ISO/IEC 27001). Seu principal objetivo é assegurar que a implementação e a manutenção de aplicativos fortaleçam a postura de segurança do Galli Group, minimizando riscos e maximizando o valor entregue aos clientes e às partes interessadas.

1.

5.19 Rede WiFi

1. **Protocolos de Criptografia Robustos:** O Galli Group determina que toda rede WiFi interna seja configurada com protocolos de criptografia modernos e seguros (como WPA2/WPA3), bloqueando, de forma preventiva, acessos

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

não autorizados e mantendo a segurança das informações em trânsito. As equipes de TI do Galli Group revisam periodicamente esses protocolos para garantir que estejam atualizados e resistentes às ameaças cibernéticas mais recentes.

2. **Segregação de Redes e Credenciais:** O Galli Group mantém o princípio de segregação de redes WiFi, separando o ambiente corporativo (restrito a colaboradores, advogados, consultores e demais credenciados) de uma eventual rede para visitantes ou fornecedores. Dessa forma, a troca de dados sensíveis nas áreas jurídicas, contábeis, financeiras, tributárias e ambientais se mantém isolada e protegida, minimizando o risco de invasões ou interceptações.

    - Cada colaborador tem suas credenciais pessoais, intransferíveis e atualizadas periodicamente.
    - Visitantes ou terceiros autorizados podem receber acesso limitado à rede, sem permissão para transitar nas redes internas do Galli Group.

3. **Monitoramento e Detecção de Anomalias:** As redes WiFi do Galli Group contam com soluções de monitoramento contínuo (e.g., sistemas de detecção de intrusão em rede wireless) para verificar tentativas de acesso indevido ou uso não autorizado. Esse monitoramento é fundamental para detectar rapidamente qualquer desvio ou anormalidade, assegurando a proteção das informações sensíveis e estratégicas no contexto do SGSI.

4. **Gestão de Senhas e Políticas de Acesso**

    - As senhas de redes WiFi são definidas conforme políticas de senhas seguras, seguindo critérios de complexidade e periodicidade de alteração estabelecidos no SGSI do Galli Group.
    - Em caso de suspeita de violação ou compartilhamento indevido de credenciais, o acesso é imediatamente revogado, e o incidente é reportado à equipe de Segurança da Informação para investigação.

5. **Atualizações e Patch Management:** Os pontos de acesso e controladores WiFi do Galli Group recebem atualizações e patches de segurança, conforme disponibilizados pelos fabricantes, garantindo que eventuais vulnerabilidades sejam prontamente corrigidas. Tais ações visam manter a robustez do ambiente sem prejudicar a disponibilidade dos serviços.

6. **Configurações de Segurança Adicionais:** Para reforçar o requisito de confidencialidade e integridade em cada unidade do Galli Group, são adotadas configurações de segurança adicionais:

    - Desativação de protocolos legados (por exemplo, WEP) e de funcionalidades de configuração automática que possam expor a rede a ataques de força bruta.
    - Políticas de ocultamento do SSID para dificultar varreduras oportunistas em áreas de alto tráfego.
    - Limitação de broadcast ao mínimo necessário, promovendo visibilidade seletiva para dispositivos autorizados.

7. **Responsabilidade dos Colaboradores e Terceiros:** Cada colaborador, prestador de serviços ou visitante com acesso às redes WiFi do Galli Group é responsável por zelar pela segurança das credenciais fornecidas, obedecendo integralmente às diretrizes desta PSI. Ao se ausentarem, os dispositivos devem permanecer protegidos, bloqueados e com antivírus ativos, evitando qualquer brecha de segurança que comprometa dados jurídicos, tributários, contábeis, financeiros ou ambientais.

5.20 Demais Recursos de TI

1. **Abrangência e Relevância:** O Sistema de Gestão da Segurança da Informação (SGSI) do Galli Group engloba, de forma abrangente, todos os dispositivos e soluções tecnológicas que possam processar, transmitir ou armazenar dados críticos ou estratégicos. Isso inclui, mas não se restringe a:

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

- Dispositivos de Impressão: Impressoras, scanners e multifuncionais, cujos registros temporários de documentos exigem cuidados especiais na manutenção de confidencialidade e descarte seguro de dados.
- Equipamentos de Videoconferência ou Audioconferência: Sistemas que possibilitam reuniões remotas devem adotar protocolos de criptografia e configurações adequadas, impedindo o acesso não autorizado a discussões sensíveis.
- Serviços de Computação em Nuvem: Aplicações e plataformas terceirizadas – utilizadas, por exemplo, no compartilhamento de documentos ou no processamento de informações — devem ser previamente avaliadas e aprovadas pela equipe de segurança do Galli Group, garantindo observância das cláusulas de confidencialidade e das legislações vigentes.
- Dispositivos de Rede Complementares (roteadores, access points, switches etc.): Embora muitas vezes não estejam diretamente associados ao processamento de dados, qualquer falha ou vulnerabilidade nesses componentes pode comprometer todo o ecossistema de segurança.
- Tecnologias de Armazenamento Móvel (pen drives, discos rígidos externos, cartões de memória): Para evitar perdas ou roubos de dados confidenciais, é fundamental controlar seu uso e aplicar criptografia adequada quando contiverem informações do Galli Group.
- Equipamentos de Backup: Sistemas e rotinas de backup são vitais para garantir a disponibilidade e a recuperabilidade das informações, sendo necessário adotar políticas de armazenamento seguro, replicação off-site e testes periódicos de restauração.

2. **Manutenção, Atualizações e Ciclo de Vida:** O Galli Group mantém processos formais de verificação e manutenção de todos esses recursos de TI, reforçando sempre o compromisso de proteger dados sensíveis e estratégicos. Dessa forma:

   - Programas de Manutenção Preventiva são estabelecidos para reduzir riscos de falhas em equipamentos, evitando possíveis interrupções que possam prejudicar as atividades das unidades de negócio (jurídica, contábil, financeira, tributária ou ambiental).
   - Atualizações de Firmware e Software são aplicadas tão logo sejam disponibilizadas, assegurando a correção de eventuais vulnerabilidades e o aprimoramento contínuo da segurança.
   - Gestão de Ciclo de Vida dos dispositivos inclui um mapeamento detalhado desde a aquisição até o descarte final, com registros apropriados, análises de risco e aplicação de boas práticas de descomissionamento, impedindo que dados críticos do Galli Group fiquem expostos ao término do uso de um recurso.

3. **Políticas Internas e Responsabilidades:** O uso de quaisquer recursos de TI no âmbito do Galli Group deve estar alinhado às diretrizes definidas na presente Política de Segurança da Informação. Assim:

   - Restrição de Acesso: Cada recurso deve ser acessado apenas por pessoas autorizadas, conforme as regras de direitos e perfis de acesso que reflitam o princípio do menor privilégio.
   - Registros e Auditorias: A equipe de segurança do Galli Group pode auditar ou monitorar o uso desses recursos para verificar a conformidade e assegurar a robustez dos controles de segurança.
   - Treinamento e Conscientização: Colaboradores e parceiros envolvidos no manuseio de dispositivos complementares (por exemplo, scanners de documentos jurídicos, equipamentos de campo para análise ambiental, ferramentas de suporte contábil e tributário) são orientados regularmente quanto às boas práticas de proteção e às consequências de uso inadequado ou negligente.

4. **Procedimentos de Emergência e Contingência:** Em situações onde ocorra falha, roubo ou qualquer evento que ponha em risco a confidencialidade ou disponibilidade de algum recurso de TI do Galli Group, os procedimentos de continuidade estabelecidos pelo SGSI deverão ser imediatamente acionados. Tais procedimentos incluem:

   - Isolamento ou Substituição do Recurso: Quando identificada a possibilidade de contaminação ou de falha iminente, o equipamento é isolado e analisado para reparo ou substituição.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

- Comunicação Imediata: A equipe de segurança e as lideranças das respectivas unidades (Galli Advogados, Fiscalli, Ambientalli, Ivaí ou Instituto Agroportuário) são informadas, visando coordenar ações de contingência e minimizar impactos nos serviços jurídicos, contábeis, financeiros, tributários ou ambientais.
- Recuperação: São empregados backups ou redundâncias para restabelecer as informações críticas e a funcionalidade do recurso comprometido.
- Registro e Análise Pós-Incidente: Concluído o tratamento emergencial, registram-se as lições aprendidas e define-se um plano de aprimoramento para fortalecer a resiliência desses recursos de TI.

5.21 Alimentos, Bebidas e Afins

1. **Proibição em Áreas Críticas:** O Galli Group determina que não sejam consumidos alimentos, bebidas ou substâncias similares (por exemplo, líquidos, sopas, refeições completas etc.) em espaços que tenham relação direta com a operação do Sistema de Gestão de Segurança da Informação (SGSI) ou que armazenem ou processem dados relevantes. Isso inclui salas de servidores, salas de arquivos confidenciais e áreas restritas destinadas ao manuseio de documentos sensíveis de clientes. A presença de tais itens pode ocasionar derramamentos e danos físicos aos equipamentos de TI, expondo o ambiente a potenciais falhas de disponibilidade ou contaminação de informações estratégicas.

2. **Áreas Designadas e Responsabilidades:** O Galli Group disponibiliza áreas designadas (como copas, refeitórios e salas de descanso) para que seus colaboradores, estagiários e visitantes possam realizar refeições ou consumir líquidos com segurança. Esses espaços são projetados para o conforto e a integração das equipes, sem comprometer a segurança das informações geridas pelas unidades Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário. É responsabilidade de cada colaborador conhecer e cumprir esta regra, assegurando que a manipulação de itens alimentícios não ocorra em locais inapropriados ou próximos a dispositivos e documentos sensíveis.

3. **Prevenção de Riscos e Continuidade de Serviços**: A ingestão de alimentos ou líquidos em áreas restritas pode acarretar riscos significativos ao SGSI do Galli Group, como curto-circuitos, interrupções no fornecimento de energia a servidores, danos irreversíveis a hardwares e, principalmente, possíveis falhas na continuidade de serviços críticos. Qualquer incidente decorrente do descumprimento destas diretrizes deve ser comunicado de imediato à equipe de segurança da informação, que avaliará o grau de impacto ao ambiente e, se necessário, acionará o plano de contingência ou continuidade de negócios aplicável.

4. **Foco em Boas Práticas e Ambiente Seguro:** Manter um local de trabalho organizado, limpo e livre de itens que possam pôr em risco os ativos de informação faz parte da cultura de segurança do Galli Group. A organização reafirma que a proteção das informações sensíveis, oriundas de suas diversas áreas de atuação, depende da observância sistemática de procedimentos simples, como evitar o consumo de alimentos em áreas críticas. Essa postura não apenas fortalece a confiabilidade das operações, mas também reflete o compromisso contínuo do Galli Group em cumprir requisitos legais e normativos, garantindo um SGSI eficaz e alinhado às melhores práticas internacionais.

5.22 Teletrabalho

1. **Ambiente Seguro e Privado:** É imperativo que o colaborador do Galli Group mantenha um ambiente seguro e privado para desempenhar suas funções em teletrabalho. Nesse sentido, devem-se evitar locais públicos ou de fácil acesso a terceiros, de modo a reduzir riscos de exposição ou divulgação indevida de dados jurídicos, contábeis, financeiros, tributários ou ambientais. Nos casos em que não haja possibilidade de um espaço isolado, o colaborador deve adotar cuidados extras para impedir a visualização acidental de informações, como uso de protetores de tela de privacidade ou posicionamento estratégico do equipamento.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

2. **Conexão Segura e Protegida:** Sempre que estiver trabalhando fora das dependências do Galli Group, o colaborador deve utilizar conexões seguras (VPN, redes confiáveis ou outros métodos de criptografia) para acessar sistemas internos, repositórios de arquivos ou aplicativos corporativos. É estritamente proibido acessar as informações do Galli Group por meio de redes públicas não criptografadas, pois isso pode comprometer a confidencialidade, a integridade e a disponibilidade dos dados.

3. **Equipamentos e Ferramentas:** Preferencialmente, o Galli Group fornece equipamentos corporativos pré-configurados para uso remoto, adequando-os às políticas de proteção da informação. Nessas máquinas, mantém-se antivírus, firewalls e outros mecanismos de segurança atualizados. Caso seja autorizado o uso de equipamentos pessoais (BYOD), é obrigatório seguir todos os requisitos de segurança definidos na PSI, especialmente no tocante a instalação de antivírus, aplicação de patches de segurança e adoção de senhas fortes e/ou autenticação multifator.

4. **Política de Senhas e Autenticação:** O colaborador em teletrabalho deve respeitar a política de senhas do Galli Group, garantindo senhas complexas, nunca as compartilhando e alterando-as periodicamente ou diante de qualquer evidência de comprometimento. Para sistemas mais sensíveis, especialmente aqueles que envolvem dados jurídicos, contábeis, financeiros, tributários e ambientais, o uso de autenticação multifator (MFA) é mandatário, quando aplicável.

5. **Proteção contra Acessos Não Autorizados:** Ao se ausentar momentaneamente do local de trabalho, o colaborador deve bloquear a tela (função "Tela Limpa") para impedir que pessoas não autorizadas visualizem dados sensíveis do Galli Group. Documentos impressos (quando estritamente necessários) devem ser armazenados em local seguro, fora do alcance de terceiros, e destruídos conforme a política de descarte de mídias e papéis confidenciais estabelecida pelo Galli Group.

6. **Reporte de Incidentes:** Qualquer incidente ou suspeita de violação de segurança (por exemplo, perda ou roubo de dispositivo, acesso não autorizado, infecção por malware) deve ser reportado imediatamente ao responsável de segurança da informação do Galli Group. O colaborador deve cooperar de maneira célere e eficaz para que as medidas corretivas sejam tomadas, preservando a confidencialidade e integridade dos dados dos clientes e das informações estratégicas das unidades.

7. **Monitoramento e Conformidade:** O Galli Group reserva-se o direito de realizar verificações e auditorias, dentro dos limites legais e contratuais, para assegurar que as práticas de teletrabalho estejam em conformidade com esta Política de Segurança da Informação. Caso sejam identificadas não conformidades, serão adotadas medidas corretivas e, se necessário, disciplinares, em função da gravidade do caso e do risco imposto às informações do Galli Group.

8. **Término do Contrato ou Migração de Atividades:** Em situações de desligamento do colaborador, rescisão de contrato ou alteração de função, as credenciais de acesso devem ser imediatamente revogadas. Quando for o caso, dispositivos corporativos devem ser devolvidos e os dados do Galli Group removidos de equipamentos pessoais (BYOD).

5.23 Visitantes

1. **Controle de Acesso:** O Grupo Galli exige que qualquer pessoa externa (visitante, fornecedor, auditor, cliente ou parceiro) seja registrada na recepção ou no ponto de controle designado antes de ingressar em qualquer ambiente físico de trabalho. Esse registro deve conter, no mínimo, dados de identificação (nome completo, documento de identidade), data e horário de entrada e saída, bem como o motivo da visita. Cada visitante recebe um crachá de identificação diferenciado, deixando claro que é um usuário externo.

2. **Acompanhamento Obrigatório:** Para proteger as informações estratégicas e sensíveis processadas no Grupo Galli, é obrigatório que os visitantes estejam sempre acompanhados por um colaborador autorizado ou pelo responsável

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

local da unidade visitada (Galli Advogados, Fiscalli, Ambientalli, Ivaí ou Instituto Agroportuário). Esse colaborador atua como anfitrião e monitora as atividades do visitante, assegurando que ele não acesse ambientes ou documentos fora do escopo da visita.

3. **Acesso Restrito a Áreas Sensíveis:** Áreas onde se manejem dados jurídicos, contábeis, financeiros, tributários ou ambientais de alta criticidade – como salas de arquivo confidencial, data centers, repositórios de processos jurídicos ou equipamentos de análise contábil e financeira – possuem restrições de acesso ainda mais rígidas. O Grupo Galli limita a permanência do visitante a esses locais somente ao tempo necessário e sob supervisão constante.

4. **Termos de Confidencialidade:** Quando um visitante, fornecedor ou parceiro tiver acesso, ainda que parcial, a informações críticas do Grupo Galli (e.g., dados de clientes, relatórios financeiros, documentação jurídica ou ambiental), torna-se imprescindível que seja formalizada a assinatura de um termo de confidencialidade (NDA). Essa exigência garante a proteção legal dos dados e reforça a responsabilidade de todos na prevenção de vazamentos e uso indevido de informações.

5. **Proibição de Gravações e Dispositivos:** A entrada de câmeras fotográficas, celulares e quaisquer outros dispositivos de gravação ou armazenamento de dados em áreas sensíveis do Grupo Galli deve seguir um procedimento de controle rigoroso. Caso seja necessário o uso de tais dispositivos para fins legítimos (por exemplo, registros técnicos em uma auditoria externa), é obrigatório obter autorização prévia do gestor da unidade, documentando o motivo e o período de uso.

6. **Etiqueta de Segurança da Informação:** É política do Grupo Galli que todos os visitantes sejam previamente orientados sobre as regras de segurança aplicáveis. O colaborador responsável pela recepção deve informar, de forma clara e objetiva, as restrições de movimentação, proibição de fotografias em áreas críticas, cuidados quanto à visualização de telas e documentos, entre outras medidas definidas no SGSI do Grupo Galli.

7. **Registro de Ocorrências:** Qualquer comportamento suspeito ou situação de risco observada durante a visita deve ser imediatamente reportada ao responsável pela segurança da informação ou ao gestor imediato da unidade em questão. O Grupo Galli possui procedimentos de investigação interna para assegurar que eventuais incidentes sejam contidos e tratados de forma eficaz.

8. **Saída e Devolução de Crachás:** Ao término da visita, é necessário que o visitante registre o horário de saída e devolva o crachá ou qualquer outro meio de identificação fornecido. Assim, mantém-se a rastreabilidade dos acessos, fundamental para a integridade do sistema de controle estabelecido pelo Grupo Galli.

5.24 Clientes

1. **Proteção de Dados de Clientes:** O Galli Group implementa barreiras tecnológicas e processuais para salvaguardar dados compartilhados pelos clientes em qualquer etapa do atendimento. Essas medidas incluem controles de acesso estritamente definidos, uso de criptografia para dados em trânsito e em repouso, monitoramento constante de atividades suspeitas, além de revisões periódicas dos processos de segurança para identificar e sanar possíveis vulnerabilidades.

2. **Transparência e Responsabilidade:** Seguindo as boas práticas de compliance e requisitos legais em vigor, o Galli Group informa de forma clara aos clientes como seus dados são coletados, processados e armazenados. A organização registra e revisa continuamente os processos de tratamento de dados, mantendo rastreabilidade nas ações executadas em sistemas críticos. Esse comprometimento com a transparência reforça a postura ética do Galli Group e solidifica a confiança entre a empresa e seus clientes.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

3. **Conformidade Jurídica e Normativa:** Consciente da importância das legislações aplicáveis, o Galli Group cumpre rigorosamente as determinações legais (como LGPD e Marco Civil da Internet) e segue normas internacionais de segurança da informação (como a ISO/IEC 27001). Essa adequação reflete o compromisso de cada unidade — Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário — em proteger os interesses dos clientes e do próprio Galli Group.

4. **Isolamento de Dados e Segmentação:** Em função da variedade de serviços oferecidos, o Galli Group adota práticas de segmentação de ambientes e bases de dados para evitar qualquer acesso indevido. Dessa forma, cada cliente se beneficia de um espaço logicamente segregado, minimizando riscos de compartilhamento acidental de informações entre diferentes escopos de atuação das unidades do Galli Group.

5. **Planos de Continuidade e Resposta a Incidentes:** Para garantir a disponibilidade dos dados e a rápida contenção de possíveis ameaças, o Galli Group mantém planos robustos de continuidade de negócios e resposta a incidentes. Esses planos definem escalonamentos, responsabilidades e fluxos de comunicação claros, assegurando que qualquer evento adverso seja prontamente tratado, com comunicação transparente aos clientes impactados e medidas eficazes de reparação.

6. **Designação de Responsáveis e Contatos:** O Galli Group, por meio de seu Encarregado de Proteção de Dados (DPO) ou equipe competente, permanece à disposição dos clientes para esclarecer dúvidas, receber solicitações referentes aos direitos dos titulares de dados e prestar apoio em eventuais demandas de auditoria ou verificação de conformidade. Esse canal de contato é parte essencial da política de proximidade e confiança que o Galli Group cultiva com sua base de clientes.

5.26 Auditoria e Monitoramento

1. **Importância da Auditoria no Galli Group:** O Galli Group considera a auditoria um instrumento fundamental para avaliar a eficácia dos controles de segurança da informação e identificar precocemente possíveis vulnerabilidades que comprometam a segurança dos dados. Por meio dessas auditorias, o Galli Group reforça a transparência interna, a aderência aos requisitos legais e o constante alinhamento às melhores práticas internacionais, como as normas ISO/IEC 27001.

2. **Escopo Abrangente de Auditoria:** As atividades de auditoria e monitoramento do SGSI do Galli Group são amplas e envolvem todas as unidades (jurídica, tributária, ambiental, contábil e financeira), garantindo uma visão completa das rotinas de segurança. Os processos de trabalho, sistemas de informação, infraestrutura de TI e equipamentos críticos do Galli Group são revisados para assegurar que as ações de proteção sejam adequadas, proporcionais aos riscos e efetivamente implantadas.

3. **Equipe Interna de Auditoria e Auditorias Externas:** O Galli Group conta com profissionais internos capacitados para realizar auditorias em intervalos planejados, o que permite uma verificação sistemática e criteriosa das políticas, procedimentos e controles técnicos estabelecidos pelo SGSI. Além das avaliações internas, o Galli Group pode contratar empresas ou organismos independentes para conduzir auditorias externas, agregando imparcialidade na identificação de não conformidades ou pontos de melhoria.

4. **Autoridade e Autonomia para Auditoria:** Os auditores do Galli Group têm liberdade para examinar registros, entrevistar colaboradores e acessar sistemas pertinentes, de modo a obter dados confiáveis e precisos sobre o cumprimento das diretrizes de segurança. Nenhum processo, equipe ou departamento do Galli Group está isento das atividades de auditoria; todos devem permitir o acesso às informações necessárias para a plena execução das avaliações.

5. **Monitoramento Contínuo para Prevenção de Incidentes:** O Galli Group implanta ferramentas de monitoramento em tempo real para mapear o tráfego de rede, os acessos a sistemas e as ações de usuários privilegiados, a fim de

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.

detectar qualquer anomalia que possa colocar em risco a segurança dos dados. Logs e indicadores-chave de desempenho (KPIs) são revisados periodicamente, visando ajustar controles e direcionar ações corretivas ou preventivas em todas as áreas de atuação do Galli Group.

6. **Resposta a Incidentes Baseada em Auditoria:** Sempre que há um incidente ou potencial vulnerabilidade detectada, o Galli Group aciona o Plano de Resposta a Incidentes. Nesse processo, as evidências geradas pelas auditorias e pelo monitoramento contínuo são utilizadas para diagnosticar a causa raiz e definir ações corretivas robustas. Após cada incidente, o Galli Group revisa seus relatórios de auditoria e monitoramento para reforçar mecanismos de proteção, agregando lições aprendidas e proporcionando melhorias contínuas na segurança da informação.

5.27 Requisitos Legais e Normativos

1. **Adesão ao Marco Civil da Internet:** O Galli Group reconhece que o Marco Civil da Internet (Lei nº 12.965/2014) estabelece diretrizes fundamentais para o uso da internet no Brasil, com ênfase na privacidade, na proteção de dados e na transparência das práticas de tratamento de informações. Sendo assim, o Sistema de Gestão da Segurança da Informação (SGSI) do Galli Group está estruturado de forma a atender aos princípios de guarda e sigilo das comunicações online, garantindo que eventuais registros, logs de acesso e demais dados digitais sejam protegidos contra usos indevidos.

2. **Conformidade com a Lei Geral de Proteção de Dados (LGPD):** O Galli Group está inteiramente alinhado aos requisitos da LGPD (Lei nº 13.709/2018), aplicando controles técnicos e organizacionais adequados para proteger dados pessoais e dados sensíveis. A coleta e o tratamento das informações ocorrem sempre a partir de bases legais claras, com transparência para clientes e partes interessadas. Cada unidade do Grupo adota procedimentos para o exercício dos direitos dos titulares de dados, tais como acesso, retificação e exclusão, conforme a legislação determina.

3. **Implementação de Normas ISO/IEC 27001:** O Galli Group estruturou seu SGSI com base nos requisitos da ABNT NBR ISO/IEC 27001, estabelecendo uma abordagem sistemática de análise de riscos, tratamento de ameaças e monitoramento contínuo. Por meio de auditorias internas e externas, o Grupo Galli comprova a robustez de seus controles, mantendo-se sempre atualizado frente às melhores práticas de gestão de segurança da informação.

4. **Atendimento a Regulamentos Setoriais:** Cada unidade do Galli Group (Galli Advogados, Fiscalli, Ambientalli, Ivaí e Instituto Agroportuário) monitora e aplica regras específicas de seus segmentos de atuação. Isso inclui normas das ordens de classe (como OAB ou CRC), bem como requisitos dos órgãos ambientais, financeiras e tributárias pertinentes. O compromisso do Grupo Galli é manter-se em total conformidade com disposições regulatórias, garantindo credibilidade e segurança.

5. **Transparência e Compromisso:** Todas as atividades e processos relacionados à segurança da informação no Galli Group são conduzidos sob o princípio de transparência, reforçando a confiança dos clientes, parceiros e autoridades competentes. O Grupo Galli empenha-se em revisar continuamente suas práticas, atualizando políticas internas, instruções de trabalho e procedimentos, de modo a refletir mudanças legislativas ou novas exigências normativas que possam surgir.

Documento de uso Restrito – protegido por regras de classificação da informação. Nenhuma parte desta publicação pode ser reproduzida, ou transmitida ou utilizada em qualquer outro meio eletrônico ou mecânico, fotocopiado, gravado ou fotografado, para outros fins sem a permissão do Grupo Galli, quando de sua propriedade.