POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

GRAZZIOTIN S/A

SUMÁRIO

1. INTRODUÇÃO

A Política de Segurança da Informação P-SI-001 é uma declaração formal da Grazziotin S/A acerca do seu compromisso com a proteção de Informações de sua propriedade ou sob sua responsabilidade, conforme definição adiante, devendo ser cumprida por todos os Colaboradores.

A Grazziotin entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos ofertados a seus clientes.

A Grazziotin S/A compreende que a manipulação da informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

Dessa forma, a Grazziotin S/A estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. OBJETIVOS

Esta Política de Segurança da Informação, tem como objetivo definir a forma adequada de gerenciar informações de propriedade ou de posse da Grazziotin S/A garantindo a confidencialidade, integridade e disponibilidade das mesmas, bem como aprimorar a segurança da informação através de diretrizes, normas e controles de segurança que permitam aos colaboradores a adoção de padrões de comportamento seguro, adequados às metas e necessidades da organização.

3. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, independentemente do nível hierárquico ou função ocupada, estagiários, aprendizes, contratados, temporários, fornecedores e terceiros, incluindo ainda qualquer indivíduo ou organização que possua vínculo com a Grazziotin S/A obedecendo ao escopo definido neste documento.

Os colaboradores com vínculo com a empresa devem ser comunicados sobre a responsabilidade em relação a Segurança da Informação no início de seu vínculo empregatício, devendo assinar o "Termo de Responsabilidade e Confidencialidade", no momento de sua contratação.

A revisão desta política será realizada anualmente pelo departamento de TI, ou sempre que houver a necessidade ou um fato relevante, de acordo com a decisão do Comitê de Segurança da Informação.

4. REFERÊNCIAS

NBR ISO 27001:2013 - Sistema de gestão de segurança da informação – Requisitos;
NBR ISO 27002:2013 - Código de prática para controles de segurança da informação;
NBR ISO 22301:2013 - Sistema de gestão de continuidade de negócios – Requisitos;

5. ESTRUTURA NORMATIVA

Os documentos que compõem a estrutura normativa da Grazziotin S/A são divididos em:

a) Política (nível estratégico): constituída do presente documento, define as regras de alto nível que representam os princípios básicos da Grazziotin S/A de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados;

b) Normas (nível tático): especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes da política;

6. NORMAS GERAIS

São os registros orientados pelas Diretrizes, de forma sucinta, das melhores práticas para a correta utilização dos ativos e recursos de Tecnologia por parte de todos os usuários, conforme as diretrizes definidas para a Política de Segurança da Informação e nas demais normas do mesmo tema, devendo ser seguida por todos aqueles abrangidos por esta política, irrestritamente. Sua principal função é consolidar de forma macro, as principais disposições existentes sobre segurança da informação.

6.1. Segurança Organizacional

A administração da Segurança da Informação é de responsabilidade da área de Tecnologia da Informação (TI), que cuida de todos os assuntos envolvendo Segurança da Informação.

Quaisquer novos recursos de processamento da informação (hardwares e/ou softwares) somente podem ser instalados no ambiente de produção com a autorização da área de TI.

Não é permitida a utilização de software não adquirido oficialmente pela Instituição, bem como suas cópias, ou de qualquer outro software, inclusive os desenvolvidos internamente, que não estejam licenciados, autorizados e homologados pela área de TI. É de responsabilidade de todos os usuários manter os aspectos de segurança e proteção das informações geradas ou custodiadas pela Instituição, de acordo com a sua classificação.

6.2. Sigilo das Informações

É de responsabilidade de todos zelar pela manutenção do sigilo das informações de sua competência e/ou conhecimentos, independentemente do meio pelo qual estejam armazenadas.

6.3. Trânsito de Informações

A Instituição pode inspecionar toda e qualquer informação (como por exemplo: arquivos, e-mails, diretórios etc.) que transite ou que esteja armazenada na sua rede, nos equipamentos de propriedade dela ou, ainda, em qualquer outro equipamento para o qual tenha, previa e expressamente, autorizado à utilização.

Todos os equipamentos colocados à disposição são para uso estritamente profissional, bem como eventuais equipamentos autorizados a este fim.

A inspeção de informações, assim como a remoção de arquivos da rede devido ao uso excessivo do recurso, só pode ser realizada por pessoa indicada e autorizada para esta atividade.

É expressamente proibido o trânsito/acesso na rede dos seguintes conteúdos:

- Material Pornográfico: é vedado o acesso, exibição, edição, cópia, armazenamento e distribuição de material de conteúdo pornográfico;
- Material Discriminatório: é vedado o acesso, exibição, edição, cópia, armazenamento e distribuição de material que expresse ou promova conteúdo discriminatório;
- Aplicativos e/ou *softwares* e/ou imagens/músicas sem licença de uso: é vedado o armazenamento, utilização e/ou distribuição de aplicações e/ou *softwares* e/ou imagens/músicas sem a devida licença de uso;
- Utilização de Mídias Removíveis sem autorização (exemplo: CD's; pendrives; smartphones; câmeras digitais etc.) tanto para entrada como para saída de dados, armazenamento, processamento, registro ou qualquer outra função afim.

6.4. Instalação ou Remoção de Equipamentos

Somente a área de TI pode instalar ou movimentar equipamentos. Nenhum equipamento pode ser retirado, no todo ou em parte, ou mesmo movimentado internamente, ainda que na mesma área, sem um prévio conhecimento e aprovação da área de TI.

Nenhum equipamento pode ingressar nas dependências da Instituição sem que haja o devido controle e registro. Isto se aplica inclusive e, principalmente, a equipamentos pessoais de fornecedores, visitantes, empregados, estagiários, terceirizados e todos os demais que, de acordo com a natureza do negócio, tenha vínculo com a Instituição.

6.5. Uso dos Recursos e Equipamentos

Os recursos de tecnologia da informação devem ser utilizados exclusivamente para as atividades da Instituição.

É de responsabilidade da área de TI zelar pelo bom estado dos recursos provendo atendimento adequado aos chamados de manutenção preventiva e corretiva, bem como controlar o inventário e a disponibilidade dos sistemas e aplicativos e demais necessidades de recursos para os usuários.

É de responsabilidade de todos os usuários o uso correto dos recursos corporativos disponibilizados, cuidando da integridade, manutenção, conservação, adequação e bom funcionamento dos recursos de informação.
É expressamente proibido:

- Uso de equipamentos de tecnologia da informação de propriedade da Instituição para fins particulares.
- Uso de equipamentos particulares, de qualquer natureza, dentro ou fora da Instituição, para fins profissionais, notadamente equipamentos com capacidade de armazenamento, processamento, transmissão/recepção de informações, sem a devida análise e autorização formal da área de TI.
- Uso de recursos de informação para prestação de serviços a terceiros.

6.6. Softwares e Aplicativos

Toda a contratação de sistemas, serviços e tecnologia devem ter uma criteriosa avaliação, levando-se em consideração requisitos de segurança, performance, custos, benefícios etc., bem como sua capacidade técnica e comercial.

A área de TI deve ser envolvida nessa análise, pois os requisitos de segurança devem ser discutidos e homologados por esta antes da disponibilização para uso.

O Gestor da área é o responsável pela solicitação de instalação de aplicativos, devendo efetivar a aceitação formal após cumprir os processos de testes e homologação para que seu uso seja disponibilizado.

6.7. E-mail Corporativo

O serviço de E-mail deve ser utilizado exclusivamente para troca de mensagens que atendam às atividades da Instituição e todo o conteúdo veiculado por e-mail deve respeitar os padrões estabelecidos pela mesma.

É expressamente proibido quanto à utilização do e-mail:

- Enviar mensagens sem identificar a origem ou utilizando-se de conta de e-mail de outras pessoas sem autorização destas.
- Enviar mensagens com conteúdo difamatório, ofensivo, discriminatório ou afins, que importune ou cause constrangimento às pessoas.

- Enviar mensagens com vírus, arquivos do tipo “Cavalo de Tróia” e mensagens não solicitadas, como spam e correntes.
- Utilizar o e-mail corporativo com o fim de comercializar produtos/serviços ou divulgar eventos que não estejam ligados à atividade da Instituição.
- Acessar a contas particulares através de Webmail (externos) ou similares, fazendo uso de recursos da Instituição, salvo se houver autorização formal da área de TI.

6.8. Internet Corporativa

A Internet é um recurso de informação fornecido com o objetivo de aumentar a produtividade dos processos de trabalho, devendo ser utilizada exclusivamente para atividades da Grazziotin.

Por se tratar de recurso disponibilizado e de uso exclusivamente profissional, a Instituição entende que pode monitorar seu tráfego e inspecionar toda e qualquer informação (como arquivos, e-mails, acesso a sites, destinatários, conteúdo etc.) que transite na sua rede ou que esteja armazenado em qualquer equipamento pertencente à mesma.

O uso de dispositivos de internet móvel nos equipamentos de propriedade da Grazziotin é proibido, exceto se previamente autorizado pela área de TI. Nos casos em que seu uso for autorizado, deve ser exclusivo para atividades da Instituição.

A troca de informação através dos mecanismos da Internet deve ser feita através de procedimentos e processos seguros devidamente analisados e aprovados previamente pela área de TI.

É expressamente proibido quanto à utilização da Internet corporativa:

- Participar em salas de bate-papo, sistema de comunicação que possibilite trafegar voz e dados pela Internet, assim como em outras mídias sociais, em nome da Instituição ou não, ou sob qualquer outra justificativa, sem autorização da área de TI.
- Utilizar recursos da Instituição para participar de jogos pela Internet ou fazer o download de qualquer natureza, que não seja de interesse profissional, como por exemplo, músicas, vídeos, filmes etc.
- Utilizar recursos da Instituição para download de arquivos, aplicativos, sistemas ou afins, ainda que shareware, freeware ou equivalentes, sem a devida autorização formal da área de TI.

6.9. Monitoramento

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Grazziotin é monitorado através de ferramentas de monitoramento, indicadores e geração de históricos:

a) Disponibilidade dos sistemas;
b) Uso da capacidade instalada de rede e dos equipamentos;
c) Latência MPLS;
d) Períodos de indisponibilidade do sistemas;
e) Indicadores de segurança do firewall;
f) Indicadores de segurança do antivírus;

6.10. Demais normas

As normativas de SI e normativas do BACEN 4.658 estão todas contidas nos documentos listados abaixo:

- N-SI-001 – Norma de Segurança em Recursos Humanos.
- N-SI-002 – Norma de Descarte Seguro.
- N-SI-003 – Norma de Segurança de Fornecedores.
- N-SI-004 - Norma de Acesso Físico ao Datacenter.
- N-SI-005 - Norma de Uso de Equipamentos.
- N-SI-006 – Norma de Gestão de Firewall.
- N-SI-007 - Norma de Desenvolvimento Seguro.
- N-SI-008 - Norma de Gestão de Patches.
- N-SI-009 - Norma de Resposta a Incidentes.
- N-SI-010 - Norma de Gestão de Vulnerabilidades.
- N-SI-011 - Norma de Logs de Auditoria.
- N-SI-012 - Norma de Backup.
- N-SI-013 - Norma de Controle de Acesso.

- N-SI-014 – Norma de Treinamento e Conscientização.
- N-SI-015 – Norma de Gestão de Antivírus.
- N-SI-016 – Norma de Prevenção a Perda de Dados.
- N-SI-017 – Norma de Detecção de Intrusão.
- N-SI-018 – Norma de Gestão de Serviços em Nuvem.
- N-SI-019 – Norma de Gestão de Riscos de Segurança da Informação.
- N-SI-020 - Norma de Classificação da Informação.

7. DIRETRIZES

As diretrizes são os pilares que abrangem todos os aspectos necessários resguardando a correta aplicação de práticas de segurança da informação; a preservação e disponibilização das informações necessárias a todos os usuários autorizados e a administração de todos os recursos de informação da forma adequada, sendo elas:

7.1. Disposições Gerais

- Proteção: proteger as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada pela Instituição.
- Responsabilidade na criação, seleção e aquisição: garantir que a criação de novos produtos, a seleção de mecanismos de segurança e a aquisição de bens levem em consideração o balanceamento dos seguintes aspectos: risco, tecnologia, qualidade, velocidade e impacto no negócio.
- Conscientização coletiva: assegurar que todos aqueles abrangidos por esta política sejam devidamente conscientizados quanto à adequação de comportamento, em face de suas responsabilidades próprias e de seus subordinados.
- Continuidade dos Negócios: garantir a continuidade dos negócios, de forma a reduzir a um período aceitável, a interrupção causada por desastres ou falhas de segurança, através da combinação de ações de prevenção e recuperação.
- Conformidade: cumprir o atendimento das leis que regulamentam as atividades da Instituição de forma a obter aderência à legislação e regulamentações aplicáveis.
- Prevenção: assegurar que providências sejam tomadas de forma a prevenir quaisquer ações ou situações que possam expor a Grazziotin S/A à perda financeira, material ou humana, direta ou indiretamente, potenciais ou reais, comprometendo seu negócio.
- Sigilo Profissional: garantir que os sistemas e informações sob sua gestão estejam sujeitos às regras referentes ao sigilo profissional, devendo garantir adequada proteção dos mesmos.

- Classificação da informação: garantir que todas as informações sejam adequadamente protegidas quanto ao seu acesso e uso, sendo que aquelas consideradas sem utilidade são destruídas no momento do seu descarte.
- Utilização dos recursos: assegurar que os recursos colocados à disposição sejam utilizados apenas para as finalidades profissionais aprovadas pela Instituição.
- Comunicação de descumprimento: comunicar à área responsável qualquer descumprimento da Política e Normas de Segurança da Informação.

8. PAPÉIS E RESPONSABILIDADES

8.1. Alta Gestão

É responsabilidade da alta gestão aprovar e apoiar a Política de Segurança da Informação assim como o desenvolvimento da cultura de segurança da a informação em toda a organização.

8.2. Diretor de TI

O Diretor de Tecnologia é o responsável por esta Política, sendo o principal responsável dentro da Empresa para tratar e responder questões de segurança da informação, bem como por implementar as regras e normas aqui estabelecidas e a sua revisão. O mesmo conta com auxílio do departamento de TI, do departamento Jurídico e do departamento de RH para manter a estrutura necessária para cumprimento desta Política.

8.3. Gestor de Segurança da Informação

- Testar a eficácia dos controles utilizados e informar ao Comitê de SI os riscos residuais;
- Definir junto do Comitê de SI, quais serviços e qual o nível do serviço, será prestado por terceiros contratados e os procedimentos e documentação de resposta aos incidentes;
- Configurar os equipamentos e sistemas de informação de uso dos Colaboradores da Empresa com os controles necessários para que se cumpra esta política;
- Implantar juntamente com a TI, registros auditáveis, que possam identificar operações realizadas, e identificar quem realizou a fim de necessidade de auditoria;

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio;
- Minimizar ao máximo o risco que sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Empresa em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros;
- Realizar auditorias periódicas de configurações técnicas e análise de riscos;
- Garantir, da forma mais rápida possível, com a integração com o sistema de RH, o bloqueio de acesso de usuários por motivo de desligamento da Empresa, ou afastamento ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Empresa;
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Empresa, mediante programa de treinamentos para os colaboradores.

8.4. Comitê de Segurança da Informação

O Comitê de Segurança da informação será composto pelo: responsável pela Segurança da Informação, Gerente de TI, Diretor de TI, e por representantes das áreas de RH, Jurídica, Financeira, Executiva e Marketing além de um representante da empresa terceirizada contratada para o suporte e monitoramento do ambiente de infraestrutura da TI tendo como objetivo a supervisão e monitoramento das políticas e normas de segurança, conforme aqui previsto.

O Comitê de Segurança da Informação se reunirá trimestralmente, ou sempre que necessário, mediante convocação por e-mail do Responsável pela Segurança da Informação, nas reuniões ordinárias, ou de qualquer de seus membros, nos demais casos.

O Comitê de Segurança da Informação deverá ser instalado, mediante autorização do mesmo, necessariamente com a presença do Responsável pela Segurança da Informação ou, na sua ausência, com um membro da Diretoria, a quem caberá a sua coordenação. As deliberações serão tomadas pelo voto da maioria dos presentes, devendo ser lavrada ata das reuniões.

8.5. Demais colaboradores

Todos os Colaboradores devem conhecer e seguir a Política de Segurança da Informação, bem como seus deveres e responsabilidades dentro da segurança corporativa da informação. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do superior imediato em caso de dúvidas, o qual recorrerá ao Gerente de TI, ou Diretor de TI ou Responsável pela Segurança da Informação, se for o caso.

Em caso de incidente que afete a segurança cibernética da Empresa, o Colaborador deverá comunicar imediatamente ao seu superior, que deverá entrar em contato com o Gerente de TI, ou Diretor de TI ou Responsável pela Segurança Cibernética. Em caso de descumprimento desta regulamentação, o Colaborador estará sujeito as sanções internas e legais previstas.

9. SANÇÕES

9.1 As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de medidas disciplinares que serão adotadas conforme ITEM 11 do código de ética e conduta da Grazziotin S/A.

9.2 A aplicação de sanções e punições será realizada conforme a análise do Comitê de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado e a recorrência, podendo o Comitê Gestor de Segurança da Informação, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

9.3 No caso de terceiros contratados ou prestadores de serviço, o CSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

9.4 Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a Grazziotin S/A, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 9.1 e 9.2 desta política.

10. GLOSSÁRIO

Alta Gestão: Grupo formado pelos diretores executivos (CEO, diretor financeiro etc.) sendo responsáveis pela tomada de decisões estratégicas que afetam toda a empresa.

Ambiente Físico: Os recursos de informática são todos os meios, nesse ambiente, pelos quais pode-se obter, gerar ou manter uma informação.

Ativo: Todo e qualquer bem tangível ou intangível pertencente, administrado ou sob responsabilidade da Instituição.

Classificação da Informação: É o nível de confidencialidade da informação, que deve ser baseada numa classificação prévia, acordada entre o proprietário da informação e os usuários.

Custódia das Informações: É a responsabilidade pela guarda das informações. A custódia não permite autorizar o acesso, nem acessar os dados sem permissão do proprietário da informação.

Comitê de Segurança da Informação: Grupo composto por representantes de várias áreas da empresa que delibera sobre assuntos relativos à segurança da informação assim como tem poder de aprovação e revisão de normas e políticas.

Ferramentas de Segurança: É o conjunto de equipamentos, programas, procedimentos e demais recursos adjacentes, usados para implantação e manutenção da segurança, como por exemplo: Antivírus, *Firewall*, VPN, IDS, Certificação etc.

Gestor Imediato: Superior imediato ou acima do colaborador da empresa.

Informação: É o conjunto de dados, imagens, textos, mídias etc., que representam os valores, situações e posições da Instituição, necessários para o funcionamento ou tomada de decisão e que produzem conhecimento. É propriedade da Instituição.

Manuseio da Informação: São as diversas formas de acesso à informação, ou seja: leitura, gravação, alteração, movimentação e eliminação de dados.

Proprietário de Informação: É a pessoa ou área responsável pela gestão da informação dentro da Instituição. O proprietário da informação é responsável pela liberação do acesso aos usuários, que efetivamente necessitam da informação, para execução do seu trabalho. É quem armazena as informações para atender as necessidades de administração e controle.

Proteção da Informação: É a necessidade de segurança que a informação deve ter contra todo o tipo de possibilidade de violação (acidental ou intencional) e destruição. É obrigatória a disponibilização de rotinas de *backup*, para serem executadas periodicamente, visando à recuperação de informações perdidas.

Recurso: Todo e qualquer bem tangível, pertencente, autorizado, administrado ou sob responsabilidade da Instituição, normalmente usados para acessar, gerar, processar, transmitir, receber, armazenar, copiar, modificar e/ou eliminar informações.

Rede de Dados: Conjunto de recursos computacionais, formado por servidores de arquivos, estações de trabalho, impressoras, roteadores e meios físicos de transmissão como *links* de comunicação e cabeamento local.

Segurança da Informação: é a preservação da confidencialidade (evitar acesso não autorizado), integridade (evitar modificação não autorizada) e disponibilidade (garantia de acesso no tempo devido).

Servidor: Equipamento específico usado para algumas finalidades bem definidas como, por exemplo, arquivamento de arquivos e dados de usuários, com regras de acesso e limites de armazenamento (servidor de arquivos), uso de e-mail (servidor de correio eletrônico), administração de uso de impressoras etc.

Usuário: É a pessoa autorizada a utilizar os serviços de informação disponibilizados em meio físico, respeitando as normas e padrões estabelecidos, inclusive os períodos delimitados.

11. REVISÕES

Esta norma é revisada com periodicidade mínima anual ou conforme o entendimento do Comitê de Segurança da Informação.

12. GESTÃO DA POLÍTICA

A política PL-**SI-001** é aprovada pelo Comitê de Segurança da Informação, em conjunto com a Diretoria da Grazziotin S/A.

A presente norma foi aprovada no dia XX/XX/2020.

Marcos Knob – Diretor de TI

Felipe Bruel - Gerente de TI

13. CONTROLE DE ALTERAÇÕES

Data	Descrição	Responsável	Versão
24/04/2020	Criação da política	Segurança da Informação	1.0
15/05/2020	Inserção de item 6.9 em norma gerais Adicionado item 8.3 em papéis e responsabilidades e atualizado item 8.4	Segurança da Informação	2.0
19/06/2020	Retirada do item 8.6 em papeis e responsabilidades e adição de alta gestão, comitê de segurança da informação e gestor imediato ao item Glossário	Segurança da Informação	3.0