Fundação GORCEIX

Política de Segurança da informação

Versão:	1
Data da versão:	02/01/2024
Criado por:	Bernardo Menicucci Grossi [Consultor Externo]
Aprovado por:	Encarregada pelo Tratamento de Dados Pessoais
Nível de confidencialidade:	Restrito

Sumário

1. Introdução

A Fundação Gorceix considera a proteção dos seus Ativos de Informação fundamental para a proteção e manutenção do seu negócio e institui a presente **Política de Segurança da Informação** como documento orientativo das diretrizes para a proteção de seus ativos e para a prevenção da sua responsabilização e de seus colaboradores.

Esta Política deve ser observada irrestritamente por todos os colaboradores diretos e indiretos da Fundação Gorceix, cumprida e aplicada internamente por todos aqueles que tenham contato com os ativos de informação da organização.
A Política de Segurança da Informação observa a legislação vigente e, em especial, a Lei 13.709/18, as boas práticas de governança de dados e a norma ABNT NBR ISO/IEC 27.002:2013.

A segurança da informação está baseada em 3 princípios: Confidencialidade, Integridade e Disponibilidade. Tais pilares estão estratificados ao longo desta Política e devem ser sempre observados com o objetivo de preservar os ativos de informação da Fundação Gorceix.

Esta Política está disponível permanentemente para consulta no Servidor interno da Fundação e qualquer esclarecimento a respeito de sua interpretação e de suas práticas podem ser obtidas diretamente no Departamento de Tecnologia da Informação - DETI ou em contato com a Encarregada pelo Tratamento de Dados Pessoais da Fundação, conforme o caso.

Contato do Setor de TI:
Amâncio Ribeiro Rezende - deti@gorceix.org.br - (31) 3559-7133

Contato da Encarregada pelo Tratamento de Dados Pessoais:
Angélica Maria dos Santos Costa – lgpd.adm@gorceix.org.br - (31) 3559-7142

2. Objetivo

A segurança da informação é considerada como o conjunto de processos e tecnologias, medidas organizacionais e comportamentais destinadas a assegurar a confidencialidade, integridade e disponibilidade da informação, sendo a sua interpretação no âmbito da Fundação Gorceix definida por esta Política.

Outras políticas, procedimentos e padrões adicionais complementam esta política. Quaisquer divergências entre o conteúdo destes documentos são resolvidas com base nesta Política.

São enumerados como objetivos básicos desta Política:

- Estabelecer as diretrizes e normas que devem ser observadas por empregados e colaboradores externos da Fundação Gorceix como comportamentos aceitáveis diante da interpretação da legislação e das boas práticas de governança de dados com o objetivo de mitigar riscos.
- Preservar a confidencialidade, integridade e a disponibilidade das informações no âmbito da Fundação Gorceix.
- Prevenir incidentes de segurança da informação e a responsabilidade da Fundação Gorceix e de seus empregados e colaboradores externos.
- Cumprir e respeitar a legislação vigente, identificar não conformidades com relação às melhores práticas de segurança da informação e oportunidades de melhoria em relação às mesmas, realizar análises críticas em relação a essas práticas e contribuir para o amadurecimento e melhoria contínua deste sistema.
- Contribuir para a continuidade das atividades da Fundação Gorceix, protegendo os seus processos internos e sistemas contra falhas sistêmicas, organizacionais ou comportamentais.
- Minimizar riscos de danos, perdas financeiras, abalo reputacional e o impacto negativo na atividade da Fundação Gorceix resultante de incidentes de segurança da informação.
- Estabelecer claramente as responsabilidades pela segurança da informação no âmbito da organização.

3. Conceitos e Definições

Ativos de Tecnologia da Informação: Todo e qualquer bem tangível ou intangível pertencente, administrado, locado ou custodiado pela Fundação Gorceix, sejam informações, sistemas ou dispositivos fixos e móveis.

Colaborador Externo: Qualquer pessoa que execute atividade profissional juntamente à Fundação Gorceix, seja ele situado internamente em suas dependências ou não, assim considerado como um terceiro que atua na organização como prestador de serviço.

Confidencialidade: É a garantia de que o acesso à determinada informação seja obtido somente por pessoas previamente autorizadas pela organização.

Disponibilidade: É a garantia de que os usuários autorizados obtenham, sempre que necessário, o acesso à informação e aos ativos correspondentes às suas atividades.

Empregado: Empregados (celetistas), Estagiários, Menores Aprendizes, Diretores e Conselheiros. Também são considerados como "colaboradores internos".

Integridade: É a garantia de que a informação seja mantida com seus atributos originais e protegida contra alterações indevidas, intencionais ou acidentais ocasionadas durante sua recepção, armazenamento ou transmissão.

4. Diretrizes

A Fundação Gorceix considera que suas informações são bens importantes. Seu uso deve ser dimensionado para divulgação correta e no tempo devido.

Na Fundação Gorceix, todos os empregados têm o dever de conhecer e cumprir essas diretrizes, como responsáveis pela preservação da confidencialidade, integridade e disponibilidade das informações, e somente sendo permitido a utilização das informações da organização para fins profissionais para a mesma.

A utilização de internet, e-mail e mídias sociais por qualquer profissional que se relaciona com a Fundação Gorceix deve ser feita de forma responsável, ética e seguir as premissas de segurança da informação, códigos de ética e postura.

O acesso a recursos e dados de Tecnologia da Informação é permitido apenas a pessoas autorizadas para fins que são estritamente ligados com as atividades da função desempenhada e as necessidades operacionais da Fundação Gorceix.

A informação corporativa pode se apresentar em diferentes formas: estratégica, conhecimento, indicador, estatística, projeto, pesquisa, ação, prática, análise, experiência, inspeção, especificação, configuração, resultado, dentre outras, e poderá existir como dados armazenados em computadores, dispositivos de armazenamento, dispositivos móveis, caixas de e-mail, escritas e/ou impressas em papel, transmitidas eletronicamente ou até em conversas.

A autorização de acesso à informação não se presume e somente se permite o acesso aos ativos necessários para o desempenho de sua função. Se houver qualquer dúvida, procure orientação.

A Política de Segurança da Informação no âmbito da Fundação Gorceix está submetida aos seguintes princípios básicos:

- Todas as normas de segurança da informação devem ser implementadas, e sua adequação e confiabilidade verificada;
- O acesso aos sistemas, aplicativos, app com informações públicas, intranet, sistema de qualidade, site e informações deve implicar na autenticação do usuário.
- O acesso deve ser autorizado apenas na medida necessária para o usuário cumprir as suas atribuições. Exceções e modificações devem ser registradas e formalizadas pelo responsável direto, ao setor de TI/Segurança da Informação;
- O proprietário da informação (Fundação Gorceix) é responsável pelas autorizações de acesso, garantindo que eles serão removidos se não mais necessários e auditados periodicamente sua adequação;
- Todos os sistemas e aplicações devem ser capazes de gerar registros adequados das atividades realizadas. Os registros devem ser ativados por meio de procedimentos adequados e autorizações;
- Ambientes de desenvolvimento, teste e produção devem ser segregados.

5. Utilização da Informação

A Fundação Gorceix monitora as informações corporativas, podendo estender ao recebimento, envio e armazenamento, utilização e manuseio, sem prévia notificação às áreas ou aos empregados, visando garantir e proteger o sigilo e a segurança das mesmas.

A utilização para outros fins e/ou divulgação de assuntos relacionados especialmente, mas não se limitando, a aspectos operacionais, comerciais, sobre clientes, sobre funcionários, jurídicos, regulatórios, financeiros, contábeis, tecnológicos, sobre marketing, comercial ou qualquer outro que se relacione às atividades da organização, obriga o empregado a obter a autorização formal e por escrito da Fundação Gorceix

O sigilo das informações é responsabilidade de todos os empregados da Fundação Gorceix.

É proibida a utilização inadequada de informações da organização, de clientes ou comentários pessoais que afetem a imagem da instituição em mecanismos de comunicação instantânea, bem como em e-mails, redes sociais ou quaisquer outros meios.

Todos os empregados que tenham acesso a informações da Fundação Gorceix, privilegiadas ou não, não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas. As restrições incluem a utilização de dados em palestras,

apresentações, publicações ou qualquer ato de divulgação para o público externo sem aprovação prévia da Diretoria.

As informações devem ser classificadas seguindo os critérios estabelecidos no apêndice desta Política.

A ausência de classificação formal ocasiona a classificação automática de "**Restrita**", devendo ser manuseadas e protegidas com cuidado compatível com sua classificação, não sendo deixadas expostas ou desprotegidas. O armazenamento das informações é realizado por tempo determinado (tabela de temporalidade) pela organização e/ou legislação vigente.

5.1. Ambiente Físico

5.1.1. Acesso e permanência de empregados e visitantes

Na Fundação Gorceix, todos empregados devem estar devidamente identificados, com uso do crachá em local visível, quando estiverem dentro do prédio administrativo, áreas comuns, Data Center e Áreas Técnicas, retirando-o ao sair das dependências.

O acesso de visitantes é de responsabilidade das áreas visitadas, cabendo zelar pela aprovação, programação e acessos aos locais, com os cuidados necessários quanto ao registro de imagens e acesso às informações por qualquer meio.

5.1.2. Acesso e permanência de empregados e visitantes / Consultores externos

Todas as pessoas que não são empregados da Fundação Gorceix mas que venham a desempenhar suas atividades internamente, como ocorre com os Consultores Externos, devem receber uma cópia deste documento, assinando um termo de ciência sobre as políticas, normas e procedimentos aplicáveis à segurança corporativa.

Quaisquer violações das regras e padrões de segurança previstos nesta Política poderão implicar em sanções de relação contratual.

5.1.3. Segurança no Ambiente de Trabalho

A Fundação Gorceix não permite a divulgação de imagens da organização, de suas instalações e de empregados identificados com crachás e/ou uniformizados, bem como o compartilhamento de informações restritas e/ou inverídicas em sites pessoais, redes sociais, aplicativos ou qualquer meio de comunicação sem sua prévia autorização por escrito.

Não é autorizada a exposição de imagem de clientes, visitantes, colaboradores externos e de empregados a não ser que seja necessário e aprovado por escrito pela pessoa e pela Diretoria, respeitando a Lei 13.709/18.

A Fundação Gorceix poderá realizar a divulgação da imagem de seus empregados nas ações de divulgação institucional relacionadas à sua atividade de acordo com a previsão legal, termo de cessão de direito de imagem e em respeito à legislação aplicável.

Não é permitido a qualquer empregado ou colaborador externo a divulgação de imagens do ambiente interno, imagens de empregados e colaboradores externos, de dados pessoais, fotografias ou de quaisquer outros registros de informações a terceiros, inclusive por meio de smartphones pessoais ou corporativos, e-mail pessoal ou corporativo, ou quaisquer outros meios assemelhados, inclusive em redes sociais, o que será considerado falta grave para os fins da relação de emprego.

Os empregados têm o dever de assegurar que informações sensíveis, tanto em formato digital quanto físico e ativos não sejam deixados desprotegidos em locais de trabalho pessoais ou públicos quando não estão em uso, mesmo que seja por um curto período de tempo ou ao final do dia.

As informações com classificação "**Restrita**" ou "**Confidencial**" deverão ser descartadas utilizando métodos que impeçam a reconstrução, tal como a utilização de fragmentadoras.

Os empregados devem zelar pela guarda e integridade das informações nos ambientes onde atuam, protegendo os locais onde existem armazenamento de informações, sejam físicas ou eletrônicas.

5.1.4. Ambiente Lógico

O acesso às informações pelos empregados, como usuários de sistemas, é restrito às necessidades inerentes ao desempenho de suas funções e atribuições e não se presume.

Não é permitida a manipulação ou a utilização de informações ou contas de acesso às quais a pessoa não tem necessidade ou direito de uso.

Usuários não autorizados que tenham acesso, ainda que transitório, a informações, dados pessoais ou outros ativos de informação da Fundação Gorceix são

pessoalmente responsáveis no âmbito civil e criminal por todas as atividades realizadas com suas credenciais de acesso.

O ambiente de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos não autorizados, garantindo a integridade, disponibilidade e confiabilidade das informações.

A Fundação Gorceix adota medidas técnicas apropriadas para prevenir que ativos de informação possam ser acessados ilegalmente, modificados sem autorização, falsificados, destruídos ou sofram interferências que afetem a confidencialidade, integridade e/ou disponibilidade das informações que eles suportam.

Os processos de implantação de sistemas de informação devem respeitar as premissas de segregação de funções e de ambientes para serem executados. Mecanismos e soluções de continuidade são identificados, definidos, implementados e mantidos para os processos de negócios considerados críticos para a Fundação Gorceix.

A Fundação Gorceix reserva para si o direito de monitorar, auditar e intervir nos acessos de dados que trafegam na internet, assim como os seus processos internos e os dados pessoais inerentes aos mesmos, de modo a salvaguardar os interesses corporativos de acordo com a lei 12.965/14 (Marco Civil da Internet) e Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais) consonantes com os objetivos dessa política.

5.1.5. Contas e senhas de acesso a sistemas

Na Fundação Gorceix toda conta de acesso a sistemas tem seu proprietário ou responsável unicamente e claramente identificado. Qualquer ação executada por intermédio de uma conta será de inteira responsabilidade de seu proprietário.

A senha de acesso de cada usuário é pessoal e intransferível, sendo o empregado, ou partes interessadas, o responsável por garantir seu sigilo.

A organização utiliza procedimentos e mecanismos de proteção e de gerenciamento de senhas que visam a manutenção da segurança das contas de acessos e informações.

As senhas de acesso aos sistemas da organização devem seguir, no mínimo, o seguinte padrão:

- Incluir números.
- Incluir letras maiúsculas e minúsculas.
- Incluir caracteres especiais que não sejam letras e números.
- Expirar a cada 180 dias.

- A nova senha não deve coincidir com as últimas 05 senhas utilizadas
- A senha deve conter, no mínimo, 08 caracteres.

A conta do usuário deverá ser bloqueada após 10 tentativas de acesso com a senha errada e permanecerá bloqueada até que o Departamento de Tecnologia da Informação - DETI realize intervenção mediante solicitação.

As solicitações de recuperação de senhas, por esquecimento ou por outro motivo, devem ser realizadas através do contato com o Departamento de Tecnologia da Informação - DETI e deverão seguir o procedimento estabelecido pelo mesmo. A senha provisória estabelecida pelo Departamento de Tecnologia da Informação – DETI, deve ser obrigatoriamente modificada no primeiro acesso.

No caso de encerramento do vínculo contratual de empregado com a Fundação Gorceix ou de eventual colaborador externo que tenha acesso a quaisquer de seus sistemas, o Departamento de Tecnologia da Informação – DETI, deve ser imediatamente comunicado a fim de que providencie **a alteração de todas as senhas de acesso,** de forma preventiva, no dia do referido desligamento e, a forneça ao Setor de Gestão de Pessoas e à respectiva liderança. para avaliação da necessidade de preservação de algum conteúdo e definição da transferência de arquivos ou apagamento integral da conta, procedimento já instruído pelo Setor de Gestão de Pessoas.

Em nenhuma hipótese será admitido o desligamento de empregado ou colaborador externo com acesso a sistema sem a inativação de seus acessos.

5.2. Perfis de acesso aos sistemas

Os perfis de acesso aos sistemas são fornecidos com base na solicitação do Setor de Gestão de Pessoas ou da Liderança responsável pela contratação, conforme o caso, e são concedidos com base nas necessidades de cada empregado, devendo ser atualizados sempre que haja transferência, promoção, remoção ou desligamento do mesmo.

5.2.1. E-mail

O e-mail corporativo é uma ferramenta de trabalho, comunicação e apoio para os processos de negócios da organização, não podendo ser utilizado para fins pessoais.

Com razão análoga, as informações de trabalho não podem ser trafegadas utilizando e-mails pessoais. O e-mail corporativo é de uso exclusivo para o exercício das suas atividades, não devendo ser utilizado para cadastro em sites comerciais, redes pessoais ou qualquer plataforma que vise a interesses particulares.

O e-mail corporativo assim considerado aquele utilizado com o domínio @gorceix.org.br é uma ferramenta de trabalho fornecida pela organização para a finalidade exclusiva vinculada à sua atividade profissional. Ele está sujeito a monitoramento realizado pelo Departamento de Tecnologia da Informação - DETI e o descumprimento das regras do contrato de trabalho e desta Política é considerada uma falta grave para os fins da relação de emprego.

O e-mail corporativo está sujeito a auditoria e monitoramento sem aviso prévio realizado pelo Departamento de Tecnologia da Informação – DETI da Fundação Gorceix.

5.2.2. Internet

A Internet também é fornecida como uma ferramenta de trabalho para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências. A Fundação Gorceix mantém regras de utilização e bloqueio de acesso a determinados sites, caixas de e-mail, conteúdos, anexos, emitentes, destinatários, assinaturas, notas, limites de tráfego e armazenamentos.

A Fundação Gorceix não autoriza a utilização dos meios de comunicação da organização para divulgar mensagens com conteúdo ilegal, pornográfico, com qualquer sentido discriminatório, de cunho religioso, raça, político-partidário, ideológico ou em desacordo com os princípios éticos e morais da organização.

Ao cadastrar no perfil das redes sociais, que é um empregado da Fundação Gorceix, o profissional não deve realizar qualquer ação que impacte a marca ou contrarie os valores da organização.

O acesso à internet na rede da Fundação Gorceix e também aquele obtido através de seus equipamentos em outras redes está sujeito a monitoramento realizado pelo Departamento de Tecnologia da Informação - DETI com o objetivo de prevenir e evitar incidentes que possam comprometer seus ativos e causar danos à sua reputação. Tanto o acesso à internet quanto os equipamentos fornecidos pela organização são ferramentas de trabalho e o uso em violação às regras desta Política é considerada uma falta grave para os fins da relação de emprego.

Alguns setores da Fundação Gorceix podem não estar sujeitos a restrição de acesso a determinados conteúdos ou sites, o que é considerado em razão de necessidades especiais para o desempenho de suas funções, mediante autorização do Responsável pela área. Porém, isso não isenta os empregados e colaboradores

externos dessas áreas de sua integral responsabilidade pelo cumprimento desta Política e pelo uso responsável dos recursos computacionais colocados à sua disposição.

O uso da internet corporativa está sujeito a auditoria e monitoramento sem aviso prévio pelo Departamento de Tecnologia da Informação - DETI da Fundação Gorceix.

5.2.3. Ativos de Processamento de Dados (Hardware e Software)

Na organização, os ativos de processamento de dados são classificados quanto a critérios de criticidade e disponibilidade para os seus negócios e processos.

Os locais que hospedam ativos de processamentos de dados têm níveis adequados e são controlados por segurança física e lógica.

Dentre as principais práticas vedadas aos empregados da Fundação Gorceix, destaca-se:

- Violação de direito autoral, segredo industrial, patente ou qualquer outra modalidade de propriedade intelectual, assim como de direitos previstos em Leis e regulamentos.
- Realizar a instalação de *patches* ou atualização de sistemas de informação sem que o Departamento de Tecnologia da Informação – DETI, assegure a prévia aquisição da respectiva licença de uso.
- Introduzir, direta ou indiretamente, programas maliciosos na rede ou servidor, tais como mas não limitados a programas de acesso remoto, vírus, cavalos de Tróia, *worms* e *ransomware*.
- Revelar as suas credenciais de acesso (login e senha) para terceiros, sejam eles internos ou externos, assim como permitir o uso de sua conta por terceiros.
- Instalar, desconectar ou mover qualquer equipamento e periférico de propriedade da organização sem aprovação por escrito da área de TI.
- Adquirir software ou hardware para uso sem prévia aprovação da área de TI.
- Degradar o desempenho dos sistemas de informação da organização.
- Contornar medidas de segurança física ou lógica estabelecidas.
- Baixar, instalar ou executar programas ou utilitários de segurança que revelem senhas, informações privadas ou explorem falhas na segurança de um sistema.
- Armazenar arquivos em pastas locais, tais como documentos, *downloads* ou *desktop,* devendo ser observada a regra de utilização do ambiente próprio no servidor corporativo.

6. Gerenciamento de Risco

Os riscos à segurança da informação são continuamente avaliados e monitorados, considerando-se as ameaças e vulnerabilidades que possam causar impactos ou danos aos processos de negócios e pessoas.

Os sistemas de proteção quanto às ameaças oriundas de ambientes externos e internos ao ambiente computacional devem ser mantidos, atualizados e monitorados.

Os riscos gerados pelos seguintes fatores devem ser avaliados: superaquecimento, fogo, fumaça, água, poeira, vibrações, agentes químicos e interrupções no fornecimento de energia. As contramedidas adequadas devem ser identificadas após a avaliação de riscos.

Os serviços de processamento e as ferramentas de comunicação necessários para a continuidade dos negócios da Fundação Gorceix devem ser protegidos contra oscilações no fornecimento de energia por meio de fontes de alimentação ininterruptas.

7. Regras de Consequência

As consequências, em caso de descumprimento destas diretrizes, serão tratadas em conformidade com o Código de Conduta e Relacionamento da Fundação Gorceix ou de acordo com o poder diretivo do empregador, conforme o caso, ou em deliberação da Diretoria mediante posicionamento das áreas envolvidas.

Qualquer pessoa que cometa os seguintes atos está sujeita a penalidades na proporção da gravidade das infrações:

- Não tomar as precauções descritas nesta política de segurança;
- Não cumprir as orientações de segurança recebidas dos responsáveis;
- Violar abertamente as medidas de proteção indicadas nas políticas de segurança;

7.1. Processo de Divulgação da PSI

A Política de Segurança da Informação deve ser de conhecimento de todos os empregados da organização e deve ser amplamente divulgada, inclusive e principalmente para novos empregados.

Os métodos de divulgação, serão:

- Campanhas internas de conscientização;
- Palestras de conscientização;
- Intranet da Fundação Gorceix;

- Ou outra mídia definida pelo setor responsável conforme necessidade da Fundação Gorceix.

8. Análise crítica da política de segurança da informação

Esta política de segurança da informação será revista a cada 12 meses através de reunião de análise crítica do Departamento de Tecnologia da Informação – DETI, juntamente com a Encarregada pelo Tratamento de Dados Pessoais da Fundação Gorceix, cuja reunião será formalizada em ata.

Toda e qualquer alteração desta Política será comunicada a todas as camadas da organização que lidem, direta ou indiretamente, com a segurança da informação ou que tenham acesso a ativos de informação da Fundação Gorceix.

8.1. Recursos humanos

Esta política deve ser constantemente objeto de treinamento e conscientização, assim como seu conhecimento deve constituir requisito para admissão.

8.1.1. Regras de segurança

Constituem regras de segurança a serem observadas irrestritamente por todos os empregados da Fundação Gorceix, juntamente com o Departamento de Tecnologia da Informação - DETI:

- Controlar as versões de programas de computador instalados e sua compatibilidade com as respectivas licenças;
- Cumprir regras de segurança para evitar contaminação por malware, ransomware e phishing scam, dentre outras práticas danosas à atividade da organização;
- Manter cópia de segurança (backup) apenas de acordo com as regras pré-definidas pela área de TI;
- Apurar, imediatamente, qualquer incidente de segurança comprovado ou de que se tenha notícia em tese.

Dentre outras atribuições inerentes à segurança da informação, o Departamento de Tecnologia da Informação – DETI, deverá estabelecer procedimentos operacionais para:

- **Detecção de invasão de sistemas e respostas.** Deve ser documentado pela área de TI, com revisão periódica anual, as medidas técnicas físicas e lógicas adotadas para evitar a invasão de sistemas e o vazamento de dados, assim como documentar a sequência de medidas adotadas para responder a comunicados de suspeitas.
- **Combate a código malicioso**. O Departamento de Tecnologia da Informação – DETI, deverá adotar medidas para prevenção de contaminação

de código malicioso nos equipamentos da Fundação Gorceix e nos equipamentos de terceiros conectados à rede, com a identificação de incidentes, medidas adotadas para a remoção do código malicioso, quarentena, perda de dados, atingimento de backup, dentre outros.

- **Gestão de invasões**. A Fundação Gorceix realizará simulações e testes periódicos para testar a capacidade de resposta a incidentes de segurança da informação de sua equipe, independentemente de aviso prévio.

Em todos os casos, o Departamento de Tecnologia da Informação - DETI e a Encarregada pelo Tratamento de Dados Pessoais, deverão apurar e documentar ações corretivas identificadas em auditoria, precisar oportunidades de melhoria e submetê-las à Diretoria para deliberação.

8.1.2. Expurgo de dados

A Fundação Gorceix estabeleceu tabela de temporalidade para a retenção de dados em seus sistemas, os quais deverão ser objeto de *backup* e expurgados quando de seu decurso, independentemente de comunicado ao usuário.
Todos os empregados ficam cientificados de que o e–mail corporativo da organização não deve ser utilizado como arquivo de documentos e que os mesmos devem zelar pelo expurgo de dados e documentos ali armazenados que estejam sujeitos à eliminação pelo encerramento do tratamento de dados pessoais ou pelo decurso do prazo de armazenamento.

Os empregados da Fundação Gorceix devem zelar pelas boas práticas de governança de dados e não utilizar o e-mail corporativo como forma de armazenamento de documentos. Afinal de contas, e-mail não é arquivo.

8.1.3. Incidente de segurança da informação

A gestão eficiente de incidentes de segurança da informação é uma questão crítica para o sucesso da atividade da Fundação Gorceix. Por este motivo, a governança de seus sistemas de informação é orientada para detectar incidentes, precisar a sua magnitude, identificar responsáveis e a extensão do mesmo, estabelecer um plano de resposta e definir responsabilidades.

8.1.4. Comunicado

O comunicado de um incidente de segurança da informação ao Departamento de Tecnologia da Informação - DETI e à Encarregada pelo Tratamento de Dados Pessoais a ser realizado pelos empregados, colaboradores externos ou quaisquer terceiros relacionados ou não à Fundação Gorceix, que do fato venham a tomar conhecimento, é um ato essencial para permitir que a organização tenha a capacidade de identificar, apurar e adotar as medidas corretivas e preventivas pertinentes.

8.1.5. Plano de resposta a incidente de segurança da informação

Diante do comunicado de um incidente de segurança da informação, o Departamento de Tecnologia da Informação - DETI e a Encarregada pelo Tratamento de Dados Pessoais se reunirão para formar a Equipe de Resposta a Incidentes, o qual consistirá no grupo de empregados abaixo designados para atuar nas respostas a serem empreendidas pela organização:

Área / Departamento	Pessoa responsável
Departamento de Tecnologia da Informação - DETI (Líder da equipe)	Amâncio Ribeiro de Rezende
Encarregada pelo Tratamento de Dados Pessoais	Angélica Maria dos Santos Costa
Assessoria de Comunicação	Eliza Peixoto
Jurídico	Telma Ribeiro de Queiroz
Compliance	Joselito Cardoso dos Santos
Superintendência	Reinaldo Otávio Alves de Brito Pinheiro
Presidência Executiva	Cristovam Paes de Oliveira

Dentre as principais responsabilidades da Equipe de Resposta a Incidentes, destaca-se:

a) Atuar para detectar e corrigir o incidente e elaborar Relatório a ser submetido à Diretoria em até 24h;
b) Elaborar Alerta, comunicado e aconselhamento aos empregados, obter aprovação da Diretoria e informar aos empregados envolvidos direta e indiretamente no incidente;
c) Educar e conscientizar os empregados da Fundação Gorceix acerca do incidente de segurança da informação e das medidas corretivas que devem ser implementadas e das oportunidades de melhoria que serão avaliadas;
d) Adotar todas as medidas necessárias para prevenir incidentes e minimizar o impacto de seus efeitos;
e) Quando for o caso, elaborar nota pública contendo informações sobre o incidente e submetê-lo à Superintendência e Presidência para aprovação.

Constituem atribuições da Equipe de Resposta a atuação na investigação da origem e das razões do incidente e avaliará, em conjunto com os respectivos gestores, a aplicação de medidas disciplinares a empregados que tenham empreendido conduta culposa ou dolosa e também coordenará e executará a comunicação da Fundação Gorceix aos órgãos competentes, assim como as ações necessárias para mitigar os efeitos e prevenir incidentes semelhantes no futuro.

A Equipe de Resposta poderá acionar empregados de outras áreas, dependendo da gravidade do incidente. Neste caso, segue abaixo uma lista das áreas que podem ser envolvidas e as suas respectivas responsabilidades:

- **Encarregada pelo Tratamento de Dados Pessoais.** É a principal instância decisória sobre o tratamento de dados pessoais e que responde diretamente à Diretoria. Terá preponderância quando o incidente envolver dados pessoais, assim definidos pela Lei 13.709/18;
- **Setor de TI**. Auxiliará na resolução de questões técnicas relacionadas ao incidente e na investigação da origem e das razões para a ocorrência do mesmo. Elaborará um laudo opinativo englobando causas diretas e indiretas e responsáveis;
- **Setor Jurídico.** Avaliará a situação decorrente do incidente e adotará as medidas apropriadas quanto aos impactos jurídicos advindos à Fundação Gorceix ou a seus empregados, clientes, parceiros comerciais ou titulares de dados pessoais afetados.
- **Setor de Compliance.** Avaliará reflexos internos do incidente em relação aos empregados, o descumprimento de políticas, conflito de interesses e recomendará a ação corretiva correspondente.
- **Setor Relações Públicas.** Avaliará o impacto do incidente na imagem da organização e estabelecerá um plano de comunicação ágil para a minimização de seus efeitos.

Ainda que alguns dos Setores acima não tenham, ao tempo do incidente, sido formalmente constituídos, a Diretoria da Fundação Gorceix designará empregados responsáveis pelo desempenho de tais funções relativamente a esta Política.

8.1.5.1. Detecção do incidente

A detecção de um incidente de forma ágil e eficiente é essencial para uma resolução bem-sucedida pela Fundação Gorceix.

São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma antecipadamente. Desta forma, todos os empregados devem se atentar aos sinais mais comuns que podem desencadear um incidente, como a invasão de rede, perda ou furto de documentos, arquivos ou dispositivos, phishing, malware, ransomware, instabilidades sistêmicas, dentre outros.

Uma vez detectado um incidente ou a mera suspeita de sua ocorrência, o empregado deverá comunicar imediatamente ao Departamento de Tecnologia da Informação – DETI, pelo e-mail deti@gorceix.org.br e a Encarregada pelo Tratamento de Dados Pessoais pelo e-mail lgpd.adm@gorceix.org.br sem prejuízo de manter seu respectivo gestor em cópia e de acionar diretamente sua liderança.

Na medida do possível, essa comunicação deverá conter:

a) Hora e data em que a suspeita do incidente foi descoberta;
b) Tipo de informações envolvidas;
c) Causa e extensão do incidente;
d) Contexto do ocorrido;
e) Qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A comunicação sobre a suspeita de um incidente é vital para a Fundação Gorceix Assim, caso o empregado suspeite de um incidente e não realize a sua comunicação, poderão ser aplicadas sanções disciplinares proporcionais à gravidade do ocorrido e à negligência do mesmo.

A identificação de incidentes de segurança da informação depende de todos e de cada um de nós. Ter conhecimento e não agir, assim como suspeitar de algo e se omitir, são consideradas faltas graves na relação de emprego e podem contribuir para a ocorrência de grandes prejuízos para a Fundação Gorceix e para todos os envolvidos. Na dúvida, comunique ao Departamento de Tecnologia da Informação - DETI e a Encarregada pelo Tratamento de Dados Pessoais.

8.1.5.2. Priorização do incidente

Uma vez que o incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à Fundação Gorceix e às pessoas envolvidas.

O impacto do incidente deverá ser auferido da seguinte forma:

Padrão de classificação do incidente	**ALTO**	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	MÉDIO	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	BAIXO	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**
		BAIXO	**MÉDIO**	**ALTO**
		Sensibilidade dos dados afetados		

Além disso, a Equipe de Resposta a Incidentes também deverá levar em consideração os seguintes critérios na classificação do incidente:

Volume de dados		Sensibilidade dos dados	
Criticidade	**Descrição**	**Criticidade**	**Descrição**
Alto	**Superior a 10% da base de dados do Grupo**	**Alto**	**Dados pessoais de crianças, adolescentes ou dados sensíveis; dados que possam gerar discriminação; dados bancários.**
Média	**Inferior a 10% e superior a 2% da base de dados do Grupo**	**Médio**	**Dados pessoais imediatamente identificáveis (ex: nome, CPF, e-mail) combinados ou não com outros dados**
Baixa	**Inferior a 2% da base de dados do Grupo**	**Baixa**	**Dados anonimizados ou pseudonimizados (desde que a chave de desanonimização não tenha sido comprometida). Dados de difícil identificação (ex: IP)**

De acordo com a matriz acima definida, a Equipe de Resposta a Incidentes deverá tomar as seguintes ações, simultaneamente ou não:

Baixa gravidade

a) Tão logo tenha ciência, trabalhar prioritariamente na solução do incidente;
b) Adotar as medidas adequadas para minimizar os efeitos causados pelo incidente e promover a sua rápida correção;
c) Formalizar a ciência da área de TI, da Encarregada pelo Tratamento de Dados Pessoais e da Diretoria;
d) Comunicar as áreas envolvidas que deverão estar à disposição da Equipe de Resposta;
e) Documentar o incidente;
f) Reunir-se para analisar o incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata que deverá ser arquivada pelo Departamento de Tecnologia da Informação - DETI e da Encarregada pelo Tratamento de Dados Pessoais, conforme o caso.

Média Gravidade

a) Tão logo tenha ciência, trabalhar de forma exclusiva na solução do incidente;
b) Adotar as medidas imediatas para minimizar os efeitos causados pelo incidente e promover a sua rápida correção. Se a correção não for possível imediatamente, adotar as medidas temporárias para minimização de riscos e danos;
c) Formalizar a ciência da área de TI, da Encarregada pelo Tratamento de Dados Pessoais e da Diretoria;
d) Comunicar as áreas envolvidas que deverão estar à disposição da Equipe de Resposta;
e) Documentar o incidente;
f) Reunir-se o mais brevemente possível para analisar o incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro devendo esta reunião ser transcrita em ata que deverá ser arquivada pelo Departamento de Tecnologia da Informação - DETI e pela Encarregada pelo Tratamento de Dados Pessoais conforme o caso;
g) Realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os empregados do incidente e das medidas preventivas que devem ser adotadas.

Alta Gravidade

a) Tão logo tenha ciência, trabalhar de forma exclusiva na solução do incidente;
b) Comunicar imediatamente a Diretoria e os gestores das áreas envolvidas os quais, em conjunto ou separadamente, deverão atuar de forma exclusiva no suporte à Equipe de Resposta e preferencialmente no mesmo local em que a mesma esteja alocada;
c) Documentar o incidente;
d) Reunir-se imediatamente para avaliar o incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata que será deverá ser arquivada pelo Departamento de Tecnologia da Informação - DETI e pela Encarregada pelo Tratamento de Dados Pessoais, conforme o caso;
e) Realizar, imediatamente, treinamento interno com todos os empregados da Fundação Gorceix para conscientizá-los sobre o incidente e medidas preventivas a serem adotadas;
f) Comunicar, imediatamente, os empregados das medidas preventivas a serem adotadas.

8.1.5.3. Incidentes que envolvam dados pessoais

Incidentes considerados relevantes e que envolvam dados pessoais devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD) em até 02 dias úteis.

A avaliação sobre quais incidentes são materialmente relevantes caberá à Encarregada pelo Tratamento de Dados Pessoais que comunicará à Diretoria da Fundação Gorceix

Caso um incidente seja identificado como relevante e a sua comunicação à ANPD seja determinada, o departamento jurídico deverá, com o apoio da Equipe de Resposta, elaborar a documentação aplicável à comunicação, a qual deverá conter, no mínimo:

a) A descrição da natureza e da categoria dos dados pessoais afetados (ex: dados sensíveis, dados de criança, dados cadastrais, dentre outros);
b) As informações aos titulares de dados pessoais envolvidos, a relação dos titulares dos dados afetados, o número de titulares afetados e o país de residência dos mesmos;
c) A indicação das medidas técnicas e de segurança utilizadas para a proteção de dados pessoais, observado o segredo comercial;
d) Os riscos relacionados ao incidente;
e) Os motivos da demora, no caso da comunicação não ter sido realizado de forma imediata;
f) As medidas que foram e também as que serão adotadas para reverter ou mitigar os efeitos do incidente.

Caso a Encarregada pelo Tratamento de Dados Pessoais determine a comunicação sobre o incidente aos titulares de dados pessoais, a área Jurídica e o Compliance irão desenvolver a mensagem de comunicação e priorizarão:

a) Os fatos ocorridos;
b) As medidas adotadas pela Fundação Gorceix para minimizar o impacto dos efeitos do incidente;
c) As eventuais medidas que possam ser tomadas pelos próprios titulares afetados para mitigar riscos; Os canais de contato para sanar dúvidas.

8.1.6. Omissões

Quaisquer situações não previstas nesta política devem ser solucionadas imediatamente pelos empregados através de consulta ao Departamento de Tecnologia da Informação - DETI e à Encarregada pelo Tratamento de Dados Pessoais.

8.1.7. Não conformidades, oportunidades de melhoria e penalidades

A periodicidade anual da revisão desta Política não impedirá a adoção de medidas de auditoria preventiva ou corretiva que se façam recomendáveis ou necessárias.
Toda e qualquer comunicação relativa ao cumprimento desta Política deverá ser feita por escrito e, preferencialmente, mediante ata de reunião assinada por todos os responsáveis.

Em qualquer caso, o não cumprimento do disposto nesta Política representará violação funcional do empregado e resultará na aplicação das sanções previstas em contrato ou na Lei.

A Fundação Gorceix observará a gravidade do ato praticado pelo seu empregado, assim como o critério de progressividade quando for o caso, para aplicar sanções que poderão consistir na orientação verbal, advertência por escrito, suspensão ou demissão por justa causa. No caso de colaborador externo, pode-se aplicar imediatamente a rescisão de seu contrato.

Todas as situações identificadas pelo Setor de TI, pela Encarregada pelo Tratamento de Dados Pessoais ou que sejam comunicadas por qualquer empregado devem ser documentadas e objeto de análise crítica.

Identificado o descumprimento desta política ou de quaisquer determinações previstas em Lei, deverão os responsáveis elaborar **Ocorrência de Não Conformidade** com o detalhamento do fato apurado, de suas causas, das consequências, das medidas corretivas realizadas, seu prazo e das penalidades aplicadas aos envolvidos.

Quando for realizada uma Ocorrência de Não Conformidade, o Departamento de Tecnologia da Informação - DETI e a Encarregada pelo Tratamento de Dados Pessoais deverão realizar auditoria preventiva ao menos uma vez no período subsequente de 06 meses e outra vez no período subsequente de 12 meses com a finalidade de verificar o cumprimento de suas determinações e adotar as medidas cabíveis.

Determinadas situações podem ser interpretadas como Oportunidades de Melhoria, assim consideradas aquelas que reflitam a adoção de melhores práticas de segurança da informação. Nesses casos, deverão o Departamento de Tecnologia da Informação - DETI e a Encarregada pelo Tratamento de Dados Pessoais documentar a Oportunidade de Melhoria e submetê-la à análise da Diretoria para a tomada de decisão. Todas as Oportunidades de Melhoria serão avaliadas anualmente para identificação da pertinência de sua aplicação.

9. Controle de alterações

10. Validade e gestão de documentos

Este documento é válido a partir de 02/01/2024.

O proprietário do documento é a Encarregada pelo Tratamento de Dados Pessoais da Fundação Gorceix, que deverá verificar e, se necessário, atualizar o documento pelo menos uma vez por ano.

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios deverão ser considerados:

- Quantidade de incidentes relacionados ao uso não aceitável ou não autorizado de ativos de informações
- Quantidade de incidentes relacionados a programas inadequados de treinamento ou conscientização de funcionários em relação à segurança de ativos de informações.

Angélica Maria dos Santos Costa
Encarregada pelo Tratamento de Dados Pessoais
Fundação Gorceix

APÊNDICE 01

CLASSIFICAÇÃO DA INFORMAÇÃO

Para que as informações sejam adequadamente protegidas, cabe ao empregado realizar a classificação quando for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

1. Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano a nenhuma organização do grupo.
2. Informação interna: informação que pode ser divulgada para os empregados do grupo, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos para a organização.
3. Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da organização ou causar impactos graves, sob o aspecto financeiro, legal e normativo.
4. Rotulagem da informação: quando se tratar de informações não públicas, devem ser rotuladas quando forem geradas, armazenadas e disponibilizadas.
5. Para informações geradas e/ou armazenadas em mídias removíveis ou papel, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.
6. Para informações geradas e mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados e eventuais Políticas de Uso associadas.
7. Em respeito à classificação da informação, todos os empregados devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.
8. Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à instituição, incluindo a internet e mídias sociais, sem prévia e expressa autorização dA Fundação Gorceix
9. Todo empregado deve respeitar o sigilo profissional e contratual. Por isso, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros empregados, fornecedores, prestadores de serviços ou demais detalhes institucionais críticos.

TERMO DE CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SIGILO

Nome:	**CPF:**
Setor/Departamento:	**Cargo:**

Declaro que tenho conhecimento da Política de Segurança da Informação e que estou ciente do seu teor, o qual está diretamente ligado ao exercício das minhas funções.

De acordo com este termo, comprometo-me a:

a) Adotar e cumprir as diretrizes indicadas na política;
b) Comunicar imediatamente o setor responsável pela segurança da informação qualquer violação desta política que seja do meu conhecimento, independentemente de qualquer juízo individual, materialidade ou relevância da violação, inclusive os casos de mera suspeita.

Estou ciente de que meus acessos físicos, lógicos, de voz e de imagem podem ser objeto de monitoramento.

Desde já, aceito, sempre que solicitado, atender e cumprir quaisquer novos itens e condições que possam vir a ser considerado partes integrantes desta política, sem a necessidade de apor assinatura em novo termo, bem como em caso de negligência ou imprudência na aplicação desta política, tenho total ciência da responsabilidade disciplinar que recairá sobre tal inobservância.

Ouro Preto, ___ de _____ de 2024.

_____

Assinatura do Empregado