Data	Versão	Elaboração	Aprovação	Descrição
01/12/2021	1.0	Ricardo Costa	Comitê de Segurança	Elaboração do documento
14/01/2023	2.0	Ricardo Costa	Comitê de Segurança	Revisão Geral do documento.

INDICE

1. OBJETIVO

Nos tempos atuais de globalização a posse da informação significa enormes oportunidades de negócios, principalmente para uma empresa como a FUNIFIER, que possui na informação o seu principal patrimônio.

Informação é um ativo que como qualquer outro, tem valor para a organização e consequentemente necessita ser adequadamente protegido.

A informação pode ser disponibilizada de várias formas, podendo ser impressa ou escrita em papéis, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos ou apresentar-se através de conversação. Seja qual for o meio pelo qual a informação é distribuída, partilhada ou armazenada, está sempre requer proteções apropriadas.

A Segurança das Informações tem a função de proteger a informação de uma série de ameaças com o objetivo de zelar pela continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades de negócios. Desta forma, a segurança das informações torna-se responsável pela preservação dos seguintes aspectos da informação:

- Confidencialidade: assegura que a informação permaneça acessível apenas a quem de direito;
- Integridade: protege a exatidão e a totalidade da informação e das possíveis formas de processamento desta;
- Disponibilidade: assegura que usuários autorizados tenham acesso à informação e aos ativos associados a ela quando necessário.

Fonte: ABNT NBR ISO/IEC 27.002

Para que a Segurança das Informações seja completamente eficaz, depende do planejamento, análise e implementação de uma série de controles, compostos por políticas, práticas, procedimentos, estruturas organizacionais ou mecanismos eletrônicos e cada um tem responsabilidade internamente.

1.1. Importância da Informação

De forma crescente os sistemas de informações têm sido expostos a uma série de ameaças, dentre as quais podemos citar apenas como exemplos, fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo e inundações.

Desta forma, podemos concluir que nos parâmetros atuais a segurança da informação é vital para a continuidade dos negócios de quaisquer organizações, bem como depende de participação ativa de todos os seus funcionários em sua implementação e monitoração.

Todas as informações criadas, manuseadas, armazenadas, transportadas ou descartadas pelos colaboradores no exercício de atividades, são de propriedade da FUNIFIER e devem ser protegidas e não divulgadas salvo quando permitidas.

1.2. A Política de Segurança

É o instrumento que contém diretrizes voltadas a auxiliar a organização, no planejamento, definição e implementação de mecanismos (normas, procedimentos, padrões, controles e outros) que guiarão e suportarão as atividades relativas à segurança das informações, nas áreas de maior risco para seus processos de negócios.

A política de segurança de informações foi definida com base nas necessidades de segurança exigidas pelos negócios da FUNIFIER, conforme relacionado:

- Documentada, adequadamente e seguida por todas as pessoas envolvidas direta ou indiretamente na execução e condução dos processos de negócios da organização;
- Revisada sempre que identificada a necessidade de adequação contínua às diversas mudanças sofridas pela organização; e
- Monitorada pelos funcionários da organização ao ponto destes serem responsáveis pelo reporte imediato e íntegro de quaisquer incidentes ocorridos.

A eficácia dos controles de segurança da informação será realizada por meio de relatórios de auditoria interna ou análise de vulnerabilidades de recursos, realizados conforme ocorram as demandas anuais.

1.3. Missão e Escopo

“Prover plataforma de gamificação, desenvolvimento, suporte, treinamento, consultoria, customização e manutenção de soluções gamificadas.”

1.4. Uso de recursos corporativos

É importante lembrar também que todo o uso de recursos de tecnologia da informação disponibilizados pela FUNIFIER tais como e-mail, sistemas, Internet, bem como fornecidos por terceiros, no uso e atribuições da FUNIFIER, devem ser utilizados estritamente para uso profissional e no interesse da FUNIFIER.

Serão considerados fins indevidos: fraudes, invasão, jogos, uso de proxys, acesso não autorizado, personificação, falsa identidade, obtenção de senhas e dados privativos, perseguição, ameaças, downloads não autorizados, distribuição de códigos maliciosos, virus, acesso e disseminação de materiais pornográficos, ofensivos, difamatório, discriminatório, preconceituoso e atentatórios à moral e aos bons costumes, instalação de softwares piratas, veiculação de opiniões político-partidárias ou religiosas, conteúdo ilegal, de incitação à violência, que não respeitem os direitos autorais ou objetivos comerciais particulares; SPAM; distribuição de correntes de mensagens eletrônicas, ações que comprometa a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela FUNIFIER, cometimento de crimes ou que venham a prejudicar, mesmo de forma não intencional, outros colaboradores, pessoas e instituições vinculadas à prestação de serviços ou recursos da FUNIFIER.

1.5. A palavra do Gestor

É obrigação de todos preservar a “confidencialidade das informações” de forma que se garanta o sigilo quando for necessário, “a integridade” de maneira que as

informações estejam sempre corretas e a “disponibilidade” para que sempre que um usuário precise de uma informação, os sistemas estejam em perfeitas condições para atendê-lo.

Em virtude destes fatores a FUNIFIER investe em recursos e padrões tecnológicos a fim de aumentar e melhorar a produtividade corporativa e de seus colaboradores, com objetivo de manter estes recursos foi elaborada uma Política de Segurança da Informação, que atende aos pré-requisitos do bom uso dos recursos computacionais da FUNIFIER.

Desta forma, problemas como vírus de computador, perda de performance, indisponibilidade de equipamentos e a necessidade de proteger a informação passam a ser tratados objetivamente, de forma a se obter os melhores resultados.

Desejo a todos que façam bom uso dos equipamentos e recursos corporativos, de maneira que a informática continue sendo uma ferramenta de evolução da Funifier.

Ricardo Lopes Costa
Sócio Administrador

2. APLICAÇÃO E DIVULGAÇÃO E ATUALIZAÇÃO

O processo de divulgação da Política de Segurança, está de acordo com os processos já adotados pela FUNIFIER na divulgação de outros documentos e políticas. A atualização, análise crítica e revisão se dará obrigatoriamente em toda análise anual através de auditorias internas, externas ou qualquer demanda de melhoria que possa surgir ou ser identificada como necessária.

Todos os envolvidos na implementação da Política de Segurança, incluindo a alta gerência, funcionários e terceiros, devem entender, conscientizar-se e comprometer-se com o conteúdo da política e de seus adendos, comprovando o atendimento a estes pré-requisitos formalmente, através da assinatura do “Termo de

Confidencialidade e Sigilo" e do "Contrato Individual Trabalho a Título de Experiência" ou até mesmo contratos de prestação de serviço ou estatutos sociais e legislação aplicável. Desta forma, o termo em questão faz parte da documentação pessoal exigida pela área de Recursos Humanos para cada funcionário, bem como dos contratos exigidos pela FUNIFIER aos terceiros e estagiários sempre que aplicável.

3. DEFINIÇÃO

- ✓ **SIG:** Sistema Integrado de Gestão;
- ✓ **SGSI:** Sistema de Gestão de Segurança da Informação;
- ✓ **Usuário:** Pessoas que usam recursos da Tecnologia da Informação;
- ✓ **S.O:** Security Office (Setor Segurança da Informação);
- ✓ **C.S.O:** Chief Security Officer (Chefe da Segurança da Informação);
- ✓ **Ativo:** Componentes da segurança da informação. Ex: Hardware, Software, pessoas, documentos e informações.
- ✓ **Segurança da Informação:** Integração de segurança física, infraestrutura tecnologia, aplicações e a conscientização, organizacional com intuito de proteger a informação.

4. RESPONSABILIDADES

S.O: Assegurar e manter esforços para melhoria do SGSI;

C.S.O: Apresentar diretrizes que assegure que as políticas do SGSI estão de acordo com os propósitos da Organização;

Gestores da Informação: Em conjunto com a área de Tecnologia da Informação, adotar mecanismos que garantam a proteção das informações sob sua gestão contra alteração, destruição, divulgação e cópia não autorizada acidentais ou intencionais; informar a área de segurança da informação sobre todas as movimentações de funcionários, terceiros/prestadores de serviços sob sua gestão.

Usuários: Conhecer e cumprir as regras relativas à segurança da informação, usando a informação e os recursos relacionados em estrita observância a esta política e aos procedimentos dela decorrentes; registrar e ou comunicar imediatamente qualquer incidente de segurança ou descumprimento a esta política que chegar ao seu conhecimento à área de Segurança da Informação.

Segurança da Informação: Implementar as regras inseridas nesta política; revogar os acessos que lhes são informados pelo Gestor do Setor; monitorar o cumprimento desta política; sempre que um incidente de segurança for detectado ou relatado, garantir que todas as ações para sua solução sejam tomadas.

Recursos Humanos: Informar a área de Segurança da Informação sobre todas as movimentações (admissões, desligamentos, transferências ou promoções) dos profissionais da FUNIFIER; garantir que todos os profissionais da FUNIFIER tenham preenchido e assinado um Termo de Confidencialidade de forma eletrônica através de plataforma on-line ou constando em contratos de prestação de serviços, Ficha de Contratação e Ficha de Desligamento bem como coletar e arquivar adequadamente os documentos.

5. DIRETRIZES

5.1 Política da Segurança da Informação

Por se tratar de um sistema integrado, a política de Segurança da Informação é integrada e se encontra nos manuais do SIG, juntamente com seus objetivos. No decorrer deste documento, será abordada uma série de políticas com o intuito de assegurar e apoiar a Segurança da Informação.

5.2 Softwares e Aplicativos

É proibido instalar, atualizar ou remover qualquer tipo de software dos computadores da FUNIFIER, bem como fazer cópias para uso externo, de softwares adquiridos ou desenvolvidos pela empresa, sem prévia autorização formal da área de Segurança da Informação e gestão.

Um software antivírus devidamente licenciado e atualizado deve ser instalado em todo e qualquer computador da empresa, tendo como padrão o uso do Windows Defender, que deve estar atualizado e poderá ser avaliado a qualquer tempo através de auditorias ou análises individualizadas, ou conforme for requerido por clientes.

5.2.1 Segregação de Funções

As credenciais de usuários devem sempre que aplicável ser segregadas por funções e atribuições adequadas a finalidade do acesso ou área de atuação do usuário, empresa ou ambiente. Periodicamente, em auditorias ou a qualquer momento que possa ser julgado necessário, revisão de direitos de acesso devem ser avaliadas e se necessário adequadas nos sistemas e recursos da Funifier.

5.2.2 Contato com autoridades e Grupos especiais

O contato com autoridades ou grupos especiais deve sempre ser mantido, seja ele para manter práticas de segurança aplicadas, requerer autorizações de funcionamento ou fornecimento e/ou qualquer outro aspecto julgado relevante. As principais autoridades, legislações e grupos de fonte de informação devem sempre ser complementados e documentados em plataforma de gestão documental e capacitação para divulgação a todos.

5.2.3 Segurança da informação na Gestão de Projetos

A segurança da informação deve ser sempre considerada na gestão de projetos, conforme metodologia de gestão de projetos institucional e avaliando sempre os riscos atrelados ao projeto.

5.2.4 Dispositivo Móvel

Todos os dispositivos móveis utilizados na Funifier, sejam eles institucionais ou particulares, com dados ou informações da empresa (sejam eles celulares, notebooks, tablets ou outros) devem ser resguardados do acesso não autorizado, para tal utilizando-se de senhas e controles de restrição de acesso. Bem como ser controlados com o uso e inclusão de dados ou informações indevidas, caso tal situação ocorra, de acordo com os termos de ética, sigilo, confidencialidade e até mesmo aplicação de sanções legais previstas ou contratuais, poderão ser aplicadas.

5.2.5 Trabalho remoto

Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto, para tal a Funifier autoriza todos os seus colaboradores a realizarem o trabalho remoto como política prioritária, porém para ter acesso a dados e recursos, todos os colaboradores devem assinar eletronicamente termos e responsabilidade institucional para evitar o mal uso de recursos, bem como a habilitação de log´s e controle transacional por usuário será aplicada para evitar ações indevidas.

5.2.6 Processo Disciplinar

Conforme processos de compliance e contratação, existem processos disciplinares formais, implantados e comunicados a todos, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação ou ações e uso indevido de dados,

recursos ou informações. Mesmo após o término de contratos a responsabilidade sobre questões éticas e de sigilo se fazem válidas.

5.2.7 Controle de ativos

O Controle de ativos institucionais será realizado conforme procedimento específico, e trará informações sobre a execução do inventário, indicação dos proprietários, informações sobre o uso aceitável (em consonância ao já informado nesta política), bem como sobre tratamento, descarte, a devolução de ativos (ao término de projetos, contratos, ou desligamentos) que será uma questão obrigatória.

5.2.8 Controle de Acessos

O Controle de acessos aos recursos institucionais da Funifier, deverá ser por acesso personificado e individualizado (com exceção de usuários administradores que possam ser necessários como para plataforma EAD/ECM e para o GITHUB, sob gestão e responsabilidade atribuída formalmente em contratos com os prestadores). Os acessos e permissões devem ser devidamente constituídos aos usuários, bem como sua revogação e atrelados as atividades e pertinência do negócio.

Usuários administradores internos deverão ser controlados e restritos, onde os acessos se darão de forma individualizada de responsabilidades, conforme apresentado:

1. EAD/ECM – Administrador Técnico
2. GitHub – Gestor da equipe de desenvolvimento/sustentação
3. Sistemas FUNIFIER – Sócio Administrador

Em relação a autenticação secreta ou de aplicativos de utilidades, podemos comentar que um único usuário utilizado é de acesso ao banco de dados, tendo apenas 2 ocorrências que podem ser mapeadas:

1. EAD/ECM – Sob responsabilidade da equipe técnica e seu gestor (visto que a conta da solução acessa diretamente ao banco de dados);
2. Ambiente de hospedagem EAD/ECM - Sob responsabilidade da empresa equipe técnica e seu administrador.
3. GitHub – Usuários individualizados na plataforma.
4. Sistemas FUNIFIER – Sócio Administrador (principalmente para ambientes de produção, que seguirão regras de divulgação conforme requerido por clientes).

Por fim, os sistemas e recursos, possuem controle por perfil de usuário e sua segregação e restrição de direitos de acesso controlados, podendo inclusive ter regras extras aplicadas ou requeridas contratualmente pelos clientes finais.

Notas:

- Datacenters recomendados com certificação ISO 27001 para implementação ao cliente.

5.2.9 Acesso a redes

Devido ao tipo de negócio da Funifier (prioritariamente de venda de software de prateleira), e do restrito grupo profissional existente, não há necessidade de constituição de uma rede corporativa interna, tendo como aspecto de qualquer forma as redes de acesso atreladas a necessidade de uso de soluções e com um nível de necessidade de restrição e controle muitas vezes menor, visto que a solução roda em rede pública (com necessidade de implementação de controles como https e avaliações de segurança).

5.2.10 Controle de acesso a Código Fonte de Programas

A restrição de controle de acesso a códigos fonte, será realizada de acordo com a metodologia de desenvolvimento, no entanto a solução e ferramenta em uso (GITHUB) permite controle de restrição e log´s de acesso ao código fonte de sistemas, rastreando e gerando informações de todas as alterações realizadas e guardando as versões.

5.2.11 Segurança Física

Os controles de segurança física aplicáveis e existentes para o negócio da Funifier são:

- Perímetros de segurança física dos ambientes operacionais principais (alocação de mão de obra);
- Perímetro de segurança física para ambientes de armazenamento e proteção de dados, se darão pela comum obrigatoriedade contratual e como prática interna na contratação de DataCenters certificados ISO 27001. Lembrando que apesar de o time de pessoas da empresa compartilhar locais ambientes e recursos, é requerido que sempre sejam ambientes com controle de acesso, câmeras de acesso, sala individualizada com controle de acesso minimamente por chave, disponibilidade de armário com chave para guarda específica de materiais locais e backups;
- Normalmente o controle de visitas como registro de ocorrências ou visitantes poderá ser realizado e registrado em formulário específico para o tema;
- O ambiente deve ter controles mínimos para reduzir a probabilidade de ameaças externas como furtos, roubos e acessos indevidos;

- Em relação ao trabalho em áreas seguras, se houver restrição de acesso em ambientes de clientes, parceiros ou de datacenter contratado, as regras de segurança da informação vigentes deverão ser cumpridas;
- Não há vulnerabilidade chave prevista devido a áreas de entrega e carregamento, devido a não aplicabilidade;
- Equipamentos que precisem ser protegidos, são protegidos desde a contratação de serviços em ambientes com controles de segurança;
- Segurança do cabeamento e de interceptação de dados deve ser avaliada sempre que utilizado um ambiente desconhecido ou não controlado para utilização de equipamentos da equipe Funifier;
- A mesma segurança aplicada aos equipamentos em ambientes da Funifier, devem ser aplicados em ambientes externos, tais como manter equipamentos em ambientes trancados, senhas, bloqueios, criptografia, antivírus ativo, dentre outros.
- Devido aos equipamentos da FUNIFIER não estarem em uma rede institucional monitorada, todos os equipamentos devem ser monitorados pelo próprio usuário sempre que necessário, em relação a acessos, senhas, vírus, etc. Podendo a empresa requerer para análise ou suporte a qualquer momento.

5.2.12 Segregação de ambientes

Os ambientes da Funifier são normalmente segregados (em várias regiões, países e com uso de grandes players mundiais), porém considerando apenas o ambiente de desenvolvimento, visto que ambientes físicos normalmente são compartilhados. Em relação ao ambiente de desenvolvimento, o ambiente de desenvolvimento é realizado em núvem com os controles de acesso e log´s do GITHUB, normalmente utilizando-se de instâncias de homologação interna em equipamento local da diretoria, ou em ambientes do cliente em ambientes de homologação e produção distintos e contratados de acordo com requisitos legais e contratuais requeridos.

5.2.13 Registros de eventos e log´s

Todos os sistemas e recursos principais da empresa (principalmente em relação a sistemas e recursos) terão log´s registrados e consultáveis, independente se de usuários comuns ou administradores. Protegidos e geridos por meio de controles terceiros dos parceiros (EAD/ECM e Desenvolvimento pelo GITHUB).

5.2.14 Sincronização de Relógios

A Sincronização de relógios será aplicada conforme padrão mundial pela região de atuação da Funifier, sendo de monitoramento de Câmeras, acessos e outros recursos de prestadores seguindo a mesma regra, podendo, no entanto, ter discrepâncias de no máximo 1 (uma) hora, como tolerância devido a horários de verão que possam ser aplicados (não sendo no entanto, aspectos relevantes a operação institucional).

5.2.15 Vulnerabilidades técnicas e auditorias

Periodicamente a Funifier poderá requerer serviços técnicos especializados para avaliar recursos e soluções institucionais em relação a práticas de mercado e aderência de práticas de segurança, sendo então formalizadas em relatórios específicos de auditorias especializadas, de forma controlada e planejada para permitir conscientemente a evolução contínua.

5.2.16 Acordos de confidencialidade e não divulgação

Todos os contratos, serviços e projetos que tenham a aplicabilidade de acordos de confidencialidade e não divulgação e sejam relevantes a questão ao negócio, devem ter tais acordos considerados.

5.2.17 Análise crítica de operações e soluções

Os processos de controle de mudanças em sistemas devem ser controlados e geridos conforme procedimento específico, mudanças em plataformas operacionais, pathches e outros recursos relevantes devem ser analisados criticamente para evitar instabilidades (o que se necessário poderá e deverá ser acompanhado inclusive periodicamente por finger prints de segurança aos principais recursos). Patches de segurança em sistemas operacionais e recursos, atualizações de soluções ofertadas, devem ser controladas em Data Centers certificados ISO 27001, previstos desde a contratação.
As ações que envolvem desenvolvimento terceirizado (como do sistema principal), devem ser monitoradas e supervisionadas. No caso da Funifier, no atual momento o diretor envolve-se diretamente desde a demanda até a validação de necessidades de ajuste.

5.2.18 Testes de segurança e aceitação

Para a solução atual, além do processo de testes interno conforme procedimento institucional, normalmente a empresa tem a obrigação de passar por crivos contratuais pelo modelo de negócio mediante POC (Prova de conceito) que avalia requisitos de segurança e funcionais, para permitir a homologação e aprovação da solução, se necessário ajustes e requisições podem chegar a ser demandadas.

5.2.19 Proteção de dados para teste

Pelo modelo de negócio, no desenvolvimento e homologação não ocorre de permitir a utilização de dados de produção, protegendo assim os dados de teste, que são selecionados com cuidado. Porém, como recomendação não é autorizado a utilização de base de produção integra, na geração de dados para teste, devem ser gerados dados com recursos de “geração de CPF” por exemplo, on-line, de forma aleatória e com dados não verídicos (sendo normalmente o cliente responsável por seus ambientes, com tenants distintos).

5.2.20 Relação com fornecedores

O relacionamento com fornecedores e parceiros se dará por processos como de Gestão de Riscos, Gestão de Projetos, Aquisições e outros. Como já apresentado, sempre que necessário cláusulas de confidencialidade e ética devem ser considerados, acordos formais devem ser estabelecidos e aspectos de segurança da informação identificados e seus respectivos riscos mapeados da cadeia de suprimentos.

5.2.21 Aspectos Legais e regulamentares

Os aspectos legais e regulamentares relativos a empresa, o negócio, soluções, serviços e prestadores, devem sempre que identificados ou julgados necessários serem considerados. Sendo documentados, mantidos e controlados através de relação formal institucional.
Direitos de propriedade intelectual também devem ser considerados, não utilizando-se de softwares, soluções ou plugins proprietários sem sua devida regularização e aquisição se necessário.

5.2.22 Proteção de Registros

Registros são protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio. Visto que o código fonte e seus log´s de atividades são gerenciados

pela empresa com uso do sistema GitHub que não permite apagar seus históricos, o mesmo acontece com o ECM/EAD.

5.2.23 Computadores e Periféricos

As credenciais de administrador do equipamentos e sistemas deverão ficar sob a guarda e responsabilidade da área de Infraestrutura ou prestadores chave responsáveis, com responsabilidade sob os recursos de sua administração como sistemas, códigos ou outros, podendo a qualquer tempo ser inclusive acionados judicialmente se necessário, restando ao usuário ao qual se destina o equipamento ou recursos/sistemas, utiliza-lo com credenciais de usuário comum, em casos especiais serão liberados conforme aprovação da Diretoria e Segurança da Informação ou do prestador chave (mediante autorização prévia).

É vedada a abertura de computadores e outros equipamentos corporativos para qualquer tipo de reparo, uma vez que, qualquer reparo necessário deverá ser feito mediante autorização formal e/ou com esforço interno, para evitar o envio indevido de equipamentos ou recursos para terceiros.

Os computadores de propriedade da FUNIFIER terão as entradas e USB´s liberadas, porém com acesso a dados sensíveis como documentos e códigos fonte controlados (ex.: pelo EAD, com Log´s e/ou GITHUB) apenas para usuários pré-cadastrados. As portas e unidades USB terão recomendação de sempre serem varridas por um antivírus antes de sua utilização, todo o contexto apresentado busca evitar que informações confidenciais da empresa sejam compartilhadas com terceiros em ambiente não monitorado e em casos especiais serão liberados conforme aprovação da Segurança da Informação.

5.2.24 Rede Corporativa

A rede interna da FUNIFIER é controlada por nuvem com acesso de usuários (ex.: GITHUB, é restrita e autorizada por grupos específicos de usuários e com log´s de atividades e acessos (permitindo o controle de versões e restauração de versões preliminares), não tendo a obrigação de um controlador de domínio próprio. A rede corporativa pelo tipo de negócio principalmente será utilizada mediante rede sem fio, que somente pode ser utilizada por equipamento da empresa, sempre sem compartilhar dados ou arquivos com a rede do prestador ou outro ambiente.

Visitantes poderão ter acesso a internet por meio da rede sem fio com controle de acesso gerenciado e sob responsabilidade do terceiro prestador, onde o controle de conteúdo não é por conta da FUNIFIER.

5.2.25 Diretórios (pastas de rede “EAD” e “Versionador SVN”)

Cada setor da FUNIFIER poderá ter seu diretório (pasta) no drive da empresa, não recomendando uso de unidades individuais e sim de estruturas e ambientes com acesso concedido e controlado pela empresa ou parceiros definidos para o recurso (ex.: EAD, GITHUB), sobre o qual terá total responsabilidade tanto no que diz respeito a gestão de acessos quanto a gestão de conteúdo, incluindo recursos geridos e controlados por terceiros.

A concessão, atribuição de perfil de acesso e a revogação de cada usuário serão efetuadas pela área/empresa prestadora responsável mediante autorização expressa do gestor da Funifier, que poderá ser comunicado por e-mail, tendo a obrigação de revisão de acesso por conta dos prestadores aos recursos (em vistas de manter as cláusulas de confidencialidade previstas contratualmente). E este que deve definir e prover o perfil de acesso correto a ser concedido a cada usuário.

A estrutura de EAD (Educação a Distância) também usada como ECM (Enterprise Content Management) localizada na nuvem e provida por prestador/parceiro é de acesso livre a todos os profissionais da FUNIFIER, porém sua utilização deve estar restrita aos propósitos de negócio e atentar para os princípios de confidencialidade, já que todo conteúdo ali colocado terá acesso irrestrito de todos os profissionais. Além disso, nenhum arquivo de utilização permanente deve ser armazenado nesta pasta, bem como exigências de clientes, devem ser seguidas as regras dos clientes (seguindo sempre que possível as melhores prática de segurança da informação).

5.2.26 Internet

Apesar da internet ser liberada, todos os funcionários são orientados quanto ao uso consciente para que não atrapalhe o andamento dos processos e atividades da FUNIFIER.

Aleatoriamente a Segurança da Informação/Direção poderá posteriormente emitir relatórios de uso da internet e para os casos em que for caracterizado o uso excessivo em sites não relacionados aos negócios da FUNIFIER o colaborador poderá ser sinalizado ou advertido individualmente, conforme termos de ética, sigilo e confidencialidade assinados.

É proibido o acesso a sites que contenham pornografia, racismo, pedofilia, jogos, violência e preconceitos em geral ou a sites que vão contra as leis vigentes.

Caso a FUNIFIER julgue necessário haverá bloqueio de acesso a arquivos e sites não autorizados, que comprometam o bom funcionamento da rede ou o desempenho e a produtividade do profissional, bem como exponham a empresa e sua estrutura à riscos de segurança.

5.2.27 Correio Eletrônico

O correio eletrônico é um recurso corporativo, colocado à disposição dos empregados e estagiários, para o desenvolvimento das atividades profissionais. Portanto, está sujeito à auditoria relativa ao uso e conteúdo.

Entre as mensagens e anexo cujo envio é proibido, destacam-se os seguintes:

- ✓ Relativo a negócios particulares;
- ✓ Propaganda comerciais, político-partidária e/ou religiosas;
- ✓ Correntes e boatos;
- ✓ Com informações que impliquem em violação de direito autoral; e
- ✓ Com conteúdo que possam comprometer a privacidade dos usuários ou o sigilo das informações.

Mensagens oriundas da Internet que não são de interesse da empresa não devem ser repassadas através do correio eletrônico corporativo. O mesmo vale para mensagens sobre vírus ou ameaças de segurança que aconselham o repasse das mensagens para outras pessoas. Nestes casos, o usuário deve eliminar a mensagem e jamais repassar internamente na empresa.

As mensagens eletrônicas dos empregados e estagiários serão identificadas com nome, cargo ou função, e telefone para contato.
Toda mensagem enviada deverá conter a seguinte informação idêntica ou similar ao final da comunicação:

“Esta mensagem pode conter informações confidenciais; somente podendo ser usada pelo indivíduo ou entidade a quem foi endereçada. A transmissão incorreta da mensagem não acarreta a perda de sua confidencialidade. Caso esta mensagem tenha sido recebida por

engano, comunique o remetente e apague-a de seu sistema imediatamente. É vedado a qualquer pessoa que não seja o destinatário usar, revelar, distribuir ou copiar qualquer parte desta mensagem. Ambiente de comunicação corporativo monitorado".

5.2.28 E-mail pessoal

É permitido ao profissional acessar seu e-mail pessoal a partir da rede da FUNIFIER, porém é proibida a utilização deste para envio ou recebimento de qualquer tipo de dado, informações ou arquivos relacionados aos negócios da FUNIFIER ou para transações em nome da mesma.

Toda e qualquer comunicação com clientes, fornecedores e outros parceiros da FUNIFIER deve ser feita, única e exclusivamente por meio do e-mail corporativo e não pelo e-mail pessoal de qualquer profissional.

5.2.29 Armazenamento em nuvem

É proibido o upload ou compartilhamento de documentos ou informações sobre a FUNIFIER para qualquer tipo de dispositivo de armazenamento em nuvem (exemplo: google drive, onedrive, dropbox) que não sejam os canais homologados para a empresa, que são:

- Diretórios de Repositórios (para backup e recuperação de dados em canais locais);
- GITHUB para controle de versionamento de código fonte;
- Ambiente EAD/ECM que controlará materiais de treinamento, documentos e registros do SGI; e
- E-mail institucional ou de parceiros.

5.2.30 Criptografia e Proteção de Ativos

Todos os dispositivos móveis devem ser protegidos contra acesso indevido, de modo que computadores portáteis devem ser criotografados e celulares devem ser protegidos com senha (quando aplicável). Os celulares usados em testes, não se aplicam esta definição devido não oferecem risco a segurança da informação.

Identificação	Ferramenta criptográfica	Algoritmo	Tamanho da chave
Backup / Dados	Backup (Pendrive e/ou EAD, GIT)	TLS 1.0	128bits

WEB /Sistemas /EAD-ECM / GitHub/ Comunicação e Dados	Pendrive, EAD, GIT	TLS 1.0	128bits
e-mail / Comunicação	SSL	SSL	128bits
Notebook (Sistema operacional / Dados)	Bitlocker para os computadores com dados sensíveis que não forem Windows Home	AES	128bits

5.2.30.1 Chaves Criptográficas e senhas

Backup: para acesso não possui arquivo de chave criptográfica, a chave é uma senha pessoal que poderá ser configurada no aplicativo, porém para restauração de backup é necessário chave criptográfica ou usuário com acesso (ex.: EAD, GITHUB);

Aplicativos WEB: o arquivo de chave criptográfica simétrica (público) e é transmitida pela web. A sua validade é definida pela entidade que a cria. E os dados trafegados usam a criptografia SSL para a conexão HTTPS.

E-mail: o arquivo de chave do e-mail é transmitido a partir da configuração do e-mail no computador; a validade é definida pela entidade que a cria e sua renovação é feita automaticamente após o vencimento.

Sistema Operacional: não possui chave criptográfica, a chave é uma senha pessoal digitada ao ligar o computador. Para dispositivos móveis (Notebook) se necessário é implementado o Bitlocker para proteção do S.O e consequentemente dos dados nele contidos (contudo, os dados principais da empresa ficam em núvem).

Sistema FUNIFIER: não possui arquivo de chave criptográfica, a chave é uma senha pessoal configurada no aplicativo. A senha é criptografada em sha256 para ser armazenada no banco de dados.

A guarda das chaves e senhas poderá ser feita através de software de gerenciamento de senha de cada aplicativo, tendo sempre que possível a recomendação de aplicar complexidade de senhas, tamanho mínimo, expiração periódica e log´s de transações habilitadas para o uso das senhas (a própria aplicação Funifier permite tais funções, porém

cada política pode ser refinada por seu cliente final). Uma cópia das chaves criptográficas, será vinculada sempre ao usuário administrador para a maioria dos recursos, que sempre que possível será personificada por usuários (com exceção do EAD/ECM que possui um "System Administrator" de responsabilidade do próprio gestor da empresa prestadora/parceira (sócio).

5.2.31 Geração de Trilhas de Auditoria (LOGS) das transações efetuadas

- As transações efetuadas deverão ser gravadas em arquivos de log.
- Os arquivos de log deverão ser gerados e revisados periodicamente.
- Os arquivos de log devem estar protegidos, de forma que não exista a possibilidade de edição/exclusão dos arquivos.
- O prazo de retenção e de consequente possibilidade de recuperação de registros nos arquivos é de 05 (Cinco) dias, contados a partir da emissão de cada registro.

5.2.32 Backup (Cópia de Segurança dos Dados) e Restore

Todos os dados de sistemas corporativos devem ser protegidos através de rotinas automatizadas de backup. O processo de Backup está definido no procedimento institucional de backup e restauração.

5.2.33 Proteção dos Dados

Os dados importantes e relevantes para o negócio da FUNIFIER devem possuir mecanismos que garantam sua adequada proteção, bem como as documentações de segurança não devem ser compartilhadas desnecessariamente.

5.2.34 Detecção e Prevenção de Intrusão, Analise de Vulnerabilidades, Detecção de Ameaças e Tratamento de Riscos de Segurança da Informação

A segurança da infraestrutura e sistemas é revalidada para garantir que o nível de mínimo de segurança seja mantido aos aspectos aplicáveis, principalmente focados as soluções. A função de monitoramento e registro de eventos deve possibilitar a prevenção e/ou detecção prematura de atividades anormais e incomuns que precisam ser tratadas, bem como a subsequente geração de relatórios no tempo apropriado.

Assegurar que medidas preventivas, detectivas e corretivas sejam estabelecidas corporativamente, em especial correções de segurança (patches) e controles de vírus, para proteger os sistemas de informação e tecnologias contra malwares (vírus, worms, spyware, Phishing, SPAM).

Os incidentes de segurança devem ser identificados, classificados, comunicados e tratados adequadamente conforme Procedimento de Gestão de Incidentes institucional. As evidências do tratamento dos incidentes devem ser preservadas.

Os Riscos de Segurança da Informação são identificados, tratados e geridos através da Matriz de Riscos.

5.2.35 Revisão de Código Seguro

Deve ser garantida a qualidade do código fonte gerado a partir do desenvolvimento, localizando possíveis erros na fase inicial do processo de desenvolvimento do código em relação principalmente a arquitetura e controle transacional.

Deve ser utilizado um processo formal de revisão no qual o código produzido seja necessariamente revisado antes de ser adicionado no repositório do projeto, preservando a segurança do código fonte, de forma que a versão implantada seja a mesma que foi homologada. Todo um processo e controle de incidentes e mudanças ocorre com uso do sistema Freedcamp, vinculado as atividades do GitHub e backupeados em bases locais com controle de versões através do Freedcamp.

5.2.36 Mesa e Tela Limpa

Para reduzir os riscos de acesso não autorizado, perda ou danos as informações durante e fora do horário de expediente, os profissionais devem seguir os critérios abaixo:

- ✓ Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente, caso contrário deverão ser destruídas ao final do dia;
- ✓ Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa;
- ✓ Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;
- ✓ Informações confidenciais devem ser mantidas em local apropriado;
- ✓ Os papéis ou mídias de computador não devem ser deixados sobre as mesas, quando não estiverem sendo usados devem ser guardados de maneira adequada, de

preferência em gavetas ou armários trancados. Seu transporte deve ser controlado, restrito e protegido do acesso indevido ou não intencional.

- ✓ Sempre que não estiver utilizando o computador não deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no setor;
- ✓ Agendas, livros ou qualquer material que possam ter informações sobre a FUNIFIER ou informações particulares devem ser guardadas em locais fechados, evitando o acesso;
- ✓ As chaves de gavetas, armários e de portas devem ser guardadas em locais fechados, evitando o acesso.

5.2.37 Instalação e Configuração Segura de Sistemas da Funifier e de Terceiros

A realização da instalação e configuração segura de Sistemas desenvolvidos pela Funifier e sistemas de terceiros deverá levar em conta os seguintes aspectos:

- ✓ Preparação do ambiente da instalação
- ✓ Estratégias de particionamento de disco
- ✓ Documentação da Instalação e Configuração
- ✓ Senhas de administrador
- ✓ Instalação mínima privilegiando utilização de recurso computacional
- ✓ Desativação de Serviços Não Utilizados
- ✓ Instalação de Correções (Patches)
- ✓ Prevenção de abuso de recursos
- ✓ Processos de validação e homologação
- ✓ Segregação de ambientes na estrutura do cliente
- ✓ Transferência de recursos e conhecimento

Para Instalação e Configuração dos Sistemas da Funifier verificar Instruções de Trabalho de Instalação e Configuração no Suporte Técnico, bem como instruções de uso, Provas de Conceito requeridas e outros aspectos.

Para softwares adquiridos de terceiros e utilizados em sistemas operacionais consideramos manter um nível de suporte contratado e metas de atendimento/entregas.

5.2.38 Plano de Continuidade dos Negócios

Para a manutenção da continuidade das atividades da FUNIFIER em casos de crises, incidentes ou desastres, foi definido o Procedimento de Gestão da Continuidade e Disponibilidade.

6. PROCEDIMENTO

O usuário obriga-se a manter o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas ou comerciais, que venham ter conhecimento ou acesso em razão do exercício de suas funções.

Não é permitido sob qualquer circunstância, divulgar, revelar, reproduzir ou fornecer informações de posse ou propriedade da FUNIFIER a entidades externas sem a aprovação da mesma.

Cada usuário é responsável pela segurança dos dados e informações que estejam sob a sua custódia e por restringir e controlar o acesso de outros usuários a ele.

A preservação e a confidencialidade das informações armazenadas em sistemas de informação serão feitas mediante a utilização de senhas e de controles de acessos por usuários.

A senha de acesso é pessoal e intransferível, permitindo de maneira clara e indiscutível o reconhecimento de qualquer usuário.

O acesso à informação será permitido de acordo com a necessidade do usuário para desempenho de suas atribuições na FUNIFIER, respeitando as regras específicas de controle de acesso.

A FUNIFIER se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, sistemas ou recursos, incluindo o acesso à internet (que poderá ser rastreado ou restrito por endereço MAC) e o uso do e-mail corporativo (individualizado).

O conteúdo desta Política e demais normativas que a apoiam deve ser conhecido e cumprido por todos os usuários, que devem obrigatoriamente notificar de forma exclusiva e imediata a área de segurança da informação em caso de suspeita de violação das regras e falha na segurança da informação.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

Uma informação é classificada como confidencial, interna ou pública de acordo com suas características conforme abaixo:

7.1 Confidencial

É toda informação associada a interesses relevantes da FUNIFIER. Se revelada, pode trazer sérios prejuízos financeiros, enorme impacto ao negócio ou repercussões para a imagem da mesma. Estas informações requerem medidas excepcionais de controle e proteção contra acessos não autorizados. As informações confidenciais devem estar obrigatoriamente classificadas, com exceção de itens que devem sempre ser considerados confidenciais que são (informações pessoais e sensíveis, código fonte de programas, estratégia comerciais e institucionais, dentre outras similares).

7.2 Interna

É toda informação cujo conhecimento e uso deve estar restrito a um grupo específico de profissionais da FUNIFIER que, pela natureza da função que exercem, são obrigados a conhecê-las. Não deve ser divulgada, publicada e estar acessível a qualquer profissional ou outros departamentos caso aplicável e com a observação.

Uma informação classificada com este nível de confidencialidade somente pode ser acessada por profissionais da FUNIFIER. As informações que não devem ser de conhecimento do público externo.

Nota: Importante ressaltar que as documentações que não tiverem classificadas, devem institucionalmente sempre ser consideradas no mínimo como internas. Principalmente documentos impressos, que serão consideradas cópias não controladas e internas.

7.3 Público

Uma informação que não possui restrição de divulgação tanto para o público interno, como para o público externo. Outra categoria além da classificação citada acima, é a informação pessoal a qual não é considerada uma classificação, mas uma designação para uma informação de natureza privada (como por exemplo dados pessoais), significando que a informação é direcionada e que somente o destinatário pode ter acesso a ela. A designação pessoal pode ser usada em combinação com qualquer outra classificação de confidencialidade.

Para a informação ser pública, ela tem de estar formalmente classificada, caso contrário, minimamente será considerada como interna.

8. EXCEÇÕES

Exceções a esta Política serão tratadas nos procedimentos específicos sobre cada um dos tópicos aqui abordados.

9. PENALIDADES

Qualquer descumprimento a esta Política será considerado uma violação do código de Conduta da FUNIFIER, e está sujeito a diversas penalidades, de acordo com a CLT - Consolidação das Leis do Trabalho.