1. OBJETIVO

Estabelecer diretrizes de segurança da informação ao Grupo Fleury, no que se refere à confidencialidade, integridade e disponibilidade de informações, para atuação segura, correta, ética e legal por todos os colaboradores do Grupo Fleury.

2. ABRANGÊNCIA

Aplicável a todas as áreas, colaboradores, médicos, terceiros e fornecedores do Grupo Fleury ou quem atue em seu nome.

3. REFERÊNCIAS

ABNT NBR ISO/IEC 27001 – Requisitos do Sistema de Gestão de Segurança da Informação – 2006;
Código de Conduta Grupo Fleury.
College of American Pathologists (CAP) Laboratory Accreditation Program (LAP) Checklist 4/6/2006 Edition.
NIST (National Institute of Standards and Technology – U.S. Department of Commerce) Special Publication 800-66, Revision 1 – An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
Norma PALC (Programa de Acreditação de Laboratórios Clínicos) Sociedade Brasileira de Patologia Clínica / Medicina Laboratorial (SBPC/ML).
Política de Comunicação.
Política de Divulgação das Informações.
Política de Gestão de Ativos.
Política de Gestão de Riscos.
SANS: Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG) – Versão 3.1 de 3 de outubro de 2011.

4. DEFINIÇÕES

Aplicação de Negócios: Software ou programa desenvolvido internamente ou por parceiros de negócio ou prestadores de serviço, especialmente desenhados para automatizar ou apoiar processos de negócio da empresa.

Central de Atendimento: Canal de atendimento e registro de demandas de TI.

Colaboradores: Todas as pessoas que atuam nas diferentes marcas e unidades de negócio do Grupo Fleury, ou seja, seus acionistas, conselheiros, diretores, gestores, colaboradores sob o regime CLT, médicos, estagiários, ou quaisquer pessoas que possam atuar em nome do Grupo Fleury.

Confidencialidade: Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.

Conta de Acesso ou *User ID*: Símbolo ou sequência de caracteres usados por um sistema para identificar um usuário específico de forma a garantir sua unicidade.

Correio Eletrônico ou e-mail: É a composição, transmissão e armazenagem de mensagens e arquivos entre usuários de sistemas de rede. Sendo transmitido via quaisquer meios eletrônicos como por exemplo por meio de protocolos de correio tais como SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*) ou IMAP (*Internet Message Access Protocol*).

Criptografia: Ciência que se dedica a transcrever dados em cifras ou códigos que poderão ser, teoricamente, lidos apenas pelo destinatário da informação.

Disponibilidade: Propriedade de manter a informação disponível para usuários autorizados, quando houver necessidade.

Dispositivos móveis: Dispositivo utilizado para transmitir e/ou armazenar dados e informações de forma eletrônica, por exemplo: CDs/DVDs, Blu-ray, pen drives, HD externo, Smartphones, Tablets, entre outros.

Gestor da Informação: Responsável pela informação e medidas necessárias à segurança e controle efetivo do acesso à informação.

Grupo Fleury: Refere-se a todas as Unidades de Negócio da Empresa.

Hardware: Unidades físicas, componentes, circuitos integrados, discos e mecanismos que compõem um computador ou os seus periféricos.

Incidente de Segurança: Qualquer evento que resulte em perda ou danos aos ativos da Organização, ou qualquer ação que desrespeite as regras de segurança.

Informação Confidencial: É uma informação sensível à estratégia ou aos negócios do Grupo Fleury, e deve ser tratada com os mesmos requisitos de segurança das informações classificadas como restritas.

Informação Interna: É uma informação cujo conhecimento e uso está restrito ao ambiente interno do Grupo Fleury, estando disponível a todos os colaboradores, bem como a fornecedores e prestadores de serviço que possuam cláusula de confidencialidade assinadas nos contratos de prestação de serviço.

Informação Pública: Informação que pode e/ou deve ser divulgada para o público externo do Grupo Fleury ou mercado.

Informação Restrita: É uma informação associada aos interesses estratégicos ou à cadeia de valor do Grupo Fleury, sendo o acesso limitado a colaboradores devidamente autorizados.

Informação sensível: A informação é considerada sensível quando ela possui detalhes comerciais, operacionais, a reputação frente aos clientes, posição ou estratégia de mercado do Grupo Fleury. Sua indisponibilidade, divulgação, alteração indevida, pode causar algum dano ou prejuízo à organização.

Informação: No presente contexto, é tudo o que se sabe sobre as atividades, propriedade ou inteligência do Grupo Fleury, seja de conhecimento de pessoas ou estejam presentes em equipamentos de TI, papéis ou em quaisquer outros meios de armazenamento, transmissão ou processamento.

Integridade: Propriedade de manter a informação exata, completa e atualizada.

Prestadores de Serviços: Pessoa ou empresa que presta serviços à organização em atividades de curta ou média duração, incluindo consultores externos, terceiros, auditores externos entre outros.

Rede Wireless: Uma rede wireless ou sem fio refere-se a uma passagem aérea sem a necessidade do uso de cabos por meio de equipamentos que usam radiofrequência (comunicação via ondas de rádio) ou comunicação via infravermelho. Incluem, mas não se limitam a equipamentos Wi-Fi e Bluetooth.

Segregação de funções (SOD *Segregation Of Duties*): Consistem na separação entre pessoas distintas das atividades conflitantes de execução, autorização, aprovação, contabilização e controle, objetivando a redução da incidência de falhas ou fraudes, independente se sua estruturação é automática ou não.

SLA – Service Level Agreement – Acordo de Nível de Serviço.

Software: Qualquer programa ou grupo de programas que instrui ao hardware sobre a maneira como ele deve executar uma tarefa, inclusive sistemas operacionais, processadores de texto e programas de aplicação.

TI: Tecnologia da Informação.

Vírus: Segmento de código ou programa que pode infectar replicar e se espalhar em sistemas computacionais sem a ação de um usuário.

5. DIRETRIZES

A informação é um ativo que como qualquer outro ativo importante é essencial para os negócios de uma organização e consequentemente necessita ser preservado e adequadamente protegido. A informação pode existir de diversas formas: pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

Seja qual for a forma em que a informação é apresentada ou o meio através do qual a mesma é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança da informação é a proteção da informação dos diversos tipos de ameaças para apoiar a continuidade e operação do negócio e pode ser obtida a partir da construção, preparação, monitoramento e análise crítica de um conjunto de controles, que incluem políticas, processos, estruturas organizacionais e tecnologias.

5.1. Normas de segurança da informação

Essa política é o principal documento que provê orientação e direcionamento das ações de segurança da informação para a elaboração de políticas, normas, procedimentos e código de conduta do Grupo Fleury alinhados com os requisitos legais e de necessidades dos negócios, contribuindo para a redução dos riscos de segurança.

As diretrizes desta política deverão ser observadas por todos os colaboradores na elaboração de procedimentos, bem como na execução de atividades e processos, tendo como escopo inicial as normas abaixo, mas não se limitando a elas:

- Controle de acesso: regular sobre controle de acesso aos principais sistemas do Grupo, padrão de senha e perfis de acesso;

- Desenvolvimento Seguro: regular os aspectos de segurança da informação no que tange a aquisição, desenvolvimento e manutenção de sistemas ou aplicações de negócios;

- Segurança da informação em infraestrutura de tecnologia: regular sobre requisitos para uma operação segura, formal, monitorada e correta dos recursos de TI. Inclui padrões de configuração segura para instalação de hardware, software e aplicativos;

- Gestão de incidentes de segurança: rescrever procedimentos para tratativas de eventos de segurança da informação permitindo a tomada de ação corretiva dentro do SLA definido na norma;

- Gestão do antivírus: regular sobre a administração, proteção e tratamento contra softwares, programas ou scripts maliciosos;

- Gestão de firewall e VPN: descrever as regras para concessão de acesso, incluindo, mas não se limitando a Colaboradores, clientes, terceiros, parceiros, prestadores de serviços, governos ou qualquer entidade externa à empresa.

- Controle de dispositivos móveis: descrever regras para controle e proteção dos dispositivos móveis do Grupo, bem como regras para autorização de uso de equipamentos terceiros dentro das

instalações do Grupo Fleury;

- Uso do Correio Eletrônico: regular sobre o uso seguro e correto do recurso de e-mail corporativo, informando sobre suas respectivas restrições de utilização;

- Gestão da Rede Wireless: definir as regras de utilização da rede sem fio, permitindo o acesso à rede corporativa apenas às pessoas elegíveis e equipamentos homologados;

- Uso da internet: definir as regras de liberação de acesso internet conforme perfis pré-estabelecidos, respeitando os princípios do código de conduta do Grupo Fleury.

- Monitoramento de Acessos: definir as diretrizes e rotinas de um processo periódico de monitoramento de determinadas ações críticas, ou ações tomadas por usuários privilegiados, realizadas em sistemas selecionados conforme a criticidade para o Grupo.

Além do descrito nas normas citadas acima, o Grupo Fleury estabelece que:

- Todas as informações e documentos criados, armazenados, transmitidos e/ou processados no ambiente do Grupo Fleury, em mídia física e/ou eletrônica, são de propriedade e/ou estão sob a custódia do Grupo Fleury, sendo vedada a divulgação parcial ou total sem prévia autorização das respectivas áreas responsáveis. Cabe aos gestores assegurar que seus respectivos colaboradores sigam essa diretriz;

- O Grupo Fleury pode receber e armazenar automaticamente informações sobre as atividades de qualquer colaborador que utilize seus recursos, incluindo, mas não se limitando a endereçamento de rede dos equipamentos, usuário, aplicativos, tela/página e conversação efetuada dentro ou por meio dos recursos disponibilizados por esta organização;

- Os prestadores de serviço e terceiros estão sujeitos às políticas internas da empresa e a todos os critérios do “Termo de Confidencialidade” que devem ser assinados no ato da contratação e, se for o caso, serão responsabilizados pelo uso indevido;

- Todo acesso privilegiado a sistemas e informações do Grupo a serem realizados por prestadores de serviço, deverão ser previamente aprovados pela área de Segurança da Informação e um Diretor Executivo;

- É proibido a todo usuário o uso ou acesso a quaisquer sistemas e aplicativos, ou mesmo a simples tentativa de acesso, aos quais não possuam autorização formal;

Dúvidas ou necessidades de informações adicionais de normas complementares e regras técnicas sobre Segurança da Informação poderão ser direcionadas para o e-mail seguranca.informacao@grupofleury.com.br.

5.2. Classificação da Informação

- As informações de propriedade ou sob custódia do Grupo Fleury, devem ser rotuladas, utilizadas, armazenadas, transmitidas e descartadas conforme o seu nível de classificação, que deve ser atribuído formalmente pelo gestor da informação;

- É vedado a qualquer colaborador à utilização indevida de informações da empresa e/ou de seus clientes, transmitirem-nas para a concorrência, utilizá-las para benefício próprio e/ou armazenar arquivos e e-mails de forma imprópria. É de responsabilidade dos gestores, assegurar que seus respectivos colaboradores cumpram com essas determinações;

- Todo acesso à informação em seu ambiente empresarial e computacional é restrito somente ao perfil de pessoas autorizadas;

- A informação poderá ser reclassificada conforme a necessidade do negócio e prazos de vigência da informação, que serão descritos em norma específica, devendo o nível de proteção ser adequado à sua classificação atual;

- É de responsabilidade de qualquer colaborador fazer o descarte de informação de modo seguro.

Na ausência de uma rotina formal de classificação da informação pelo Grupo, os cargos de gestão

da empresa serão responsáveis pela exigência da proteção adequada das informações, conforme conteúdo nela existente.

As informações de acordo com o nível de classificação (Ver item 4. Definições) deverão ser submetidas aos seguintes controles:

a) Confidencial

Além de controles adicionais para evitar o acesso não autorizado, invariavelmente, tais controles devem incluir ao menos uma criptografia para transmissão ou armazenamento. Cabe ao responsável pela geração desse tipo de informação, identificá-la como tal.

Informações confidenciais não devem ser impressas sem que existam controles de segurança que garantam a sua confidencialidade durante todo o seu ciclo de vida. A divulgação de informações confidenciais deve seguir as diretrizes descritas no item 5.3 desta política.

b) Restrita

Estas informações requerem medidas de controle e proteção contra acessos, cópias, reproduções, alterações ou divulgação não autorizadas. Cabe ao responsável pela geração desse tipo de informação, identificá-la como tal.

c) Interna

Devem ser empregadas medidas para a preservação dessa informação no ambiente da empresa. Toda informação que não estiver formalmente identificada, deverá ser classificada como interna.

d) Pública

Sem implicações de proteção e controles de acesso para a manutenção da confidencialidade, contudo, a disponibilidade e integridade devem ser preservadas. Cabe ao responsável pela geração desse tipo de informação, identificá-la como tal.

5.3. Divulgação de Informação Confidencial

- Toda negociação ou contrato com qualquer fornecedor só poderá ser iniciada após assinatura de clausulas de confidencialidade, que serão parte integrante do contrato;

- Informações confidenciais só podem ser reveladas a terceiros após a assinatura de um termo específico de confidencialidade entre as partes, o qual deverá estar em conformidade com o modelo pré-estabelecido pelo Departamento Jurídico do Grupo Fleury;

- As informações devem ser protegidas desde sua origem ou criação até a sua destruição (ciclo de vida);

- Quando fora de uso, documentos ou outras mídias que contenham informações sensíveis devem ser mantidos em local seguro (caixa forte, arquivo fechado ou outra solução que garanta a segurança necessária), bem como cópias de segurança armazenadas em instalações externas. É de responsabilidade de cada colaborador, recolher de cima das suas respectivas mesas de trabalho ao final de expediente, documentos ou materiais sensíveis;

- A impressão de informações confidenciais deve ser controlada e monitorada. Quando impressas, as informações confidenciais devem ter a primeira e a última página com folha de rosto e tais folhas não podem ser removidas, de modo a proteger o conteúdo impresso. De preferência, estas informações devem ser fixadas em pastas, logo depois de impressas, para que as folhas não se extraviem, ou seja, extraviadas;

- Durante o armazenamento digital, a informação confidencial deve estar criptografada e as chaves de criptografia devem ser guardadas de forma segura, preferencialmente dividida em partes com custódia compartilhada;

- Durante a transmissão, as informações confidenciais devem ser criptografadas utilizando protocolos específicos para este fim.

O colaborador é responsável por observar e seguir as 7 (sete) determinações, acima citadas, referentes à divulgação de informação confidencial, competindo ao seu gestor imediato a garantia

do cumprimento das mesmas.

5.4. Ações e Sanções

- Qualquer colaborador deve comunicar imediatamente a Área de Segurança da Informação caso identifique a violação desta política ou demonstração de conduta que perturbe o funcionamento normal da rede, dos sistemas, dos processos ou dos negócios do Grupo Fleury, seja de forma maliciosa ou não intencional;

- Descumprimentos de políticas e normas do Grupo Fleury são passiveis de punição. Os procedimentos definidos no Código de Conduta devem ser aplicados nestas ocorrências;

- As ocorrências de violação de regras não contempladas no Código de Conduta são passiveis de medidas educativas alinhadas com o superior imediato do colaborador ou gestor do contrato em questão.

5.5. Disposições Gerais

- Esta política encontra-se em fase de implantação através da área de Segurança da Informação, e alguns itens descritos serão implementados gradativamente. Os casos de aplicabilidade serão avaliados pelo Comitê de Segurança;

- Esta política deve ser revisada anualmente, ou caso haja alteração significativa nas diretrizes de segurança da informação, com o objetivo de manter-se atualizada quanto às mudanças inerentes de tecnologias, processos e necessidade de negócio e de segurança da informação.

6. RESPONSABILIDADES

6.1 Todos colaboradores:

- Devem ter conhecimento da Política de Segurança de Informação e ser coerente com o mesmo;

- Devem manter em sigilo suas Identidades digitais e senhas de rede ou em aplicativos fornecidos, sendo as mesmas de uso pessoal e intransferível e cada colaborador será responsável pela sua guarda e uso das mesmas, assim o compartilhamento de senha é considerado falta grave e passível de sanção conforme previsto no código de conduta;

- Devem respeitar e manter a confidencialidade, integridade e disponibilidade das informações do Grupo Fleury e de seus clientes, parceiros e fornecedores;

- Devem utilizar as autorizações, as informações e os ativos fornecidos ou disponibilizados pelo Grupo Fleury, exclusivamente para a execução das atividades atribuídas às suas funções ou atribuições;

- Devem informar qualquer suspeita de violação de segurança, bem como todos os incidentes ocorridos, à área de Segurança da Informação;

- Devem participar dos programas de treinamento e conscientização sobre segurança da informação;

6.2 Coordenadores, Gerentes e Diretores:

- São responsáveis pelo direito de acesso lógico e físico dos Colaboradores e terceiros sob sua responsabilidade, devendo informar imediatamente a área de TI através Central do Atendimento, sobre eventuais trocas dos direitos de acessos, transferências e mudanças de funções e revogação de acesso, de todos os sistemas que os colaboradores e terceiros sob sua gestão tenha acesso;

- Devem avaliar criteriosamente antes de aprovar solicitações de acesso às informações e recursos do Grupo Fleury, sistemas ou aplicações específicas para seus Colaboradores, de forma que não comprometa a segurança das informações da empresa com liberação de permissões que vão além das necessidades das atividades de trabalho exercidas (Princípio do Privilégio Mínimo, ou seja, acesso somente às aplicações e níveis de alçada necessários), sendo responsabilidade do gestor os riscos envolvidos aos acessos liberados indevidamente;

- Devem assegurar que todos os Colaboradores sob sua gestão conheçam as atribuições e

responsabilidades relativas à segurança da informação;

- Devem gerir e fiscalizar as atividades executadas pela equipe relacionadas à segurança da informação, para possibilitar a identificação e o reporte do uso incorreto ou malicioso das informações, recursos ou ativos do Grupo Fleury.

6.3 Administradores de Ativos de TI e Desenvolvedores:

- Devem administrar e garantir a disponibilidade, integridade e confidencialidade de todos os ativos e informações sob sua responsabilidade ou de seus sistemas;

- Devem utilizar de forma responsável, profissional, ética, legal e aderente as diretrizes de seguranças definidas por esse documento, os direitos de acesso privilegiado sob sua responsabilidade;

- Devem administrar o acesso lógico aos sistemas sob sua responsabilidade, garantindo que os Colaboradores tenham acesso somente às informações e recursos previamente autorizados;

- Apoiar atividades de auditoria ou monitoramento quanto ao funcionamento ou configuração dos ativos, processos ou sistemas sob sua responsabilidade, incluindo, mas não se limitando às contas de acesso, logs, configurações e eventos;

- Formalizar e reportar à Área de Segurança da Informação qualquer risco identificado durante a execução das suas atividades, que não tenham sido adequadamente tratadas ou reconhecidas pelos seus demandantes ou superiores;

- Providenciar, ou solicitar às áreas competentes, que implementem controles apropriados para prevenir que os registros sejam desativados, modificados ou apagados, ou que os sistemas sejam utilizados de modo incorreto;

- Realizar backup antes de modificações realizadas nos sistemas. Documentar toda e qualquer modificação realizada no ambiente de produção;

- Não permitir cópias do Banco de Dados do ambiente de Produção para ambientes de Teste ou Homologação, sem a validação prévia da área de Segurança da Informação;

- Ao final do vínculo empregatício e/ou contratual, de seus colaboradores, desativar as identidades digitais utilizadas por estes durante o vínculo ou prestação de serviço.

6.4 Área de Segurança da Informação:

- Definir, documentar, manter e publicar as políticas e procedimentos relacionados à segurança da informação, de acordo com a governança normativa do Grupo Fleury;

- Analisar e revisar as ITR's de segurança pelo menos uma vez por ano, atualizando conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente do Grupo Fleury;

- Fornecer requisitos, controles, orientações e melhores práticas de segurança da informação aos interessados ou sempre que necessário. Isto inclui, mas não se limita à:

    - ✓ Participação em Projetos e processos (de TI ou de negócios)
    - ✓ Orientações para a configuração segura de hardware, software e redes (incluindo redes wireless);
    - ✓ Auxílio na aplicação de correções de segurança;
    - ✓ Orientações de como administrar contas de acesso;
    - ✓ Boas práticas de segurança no ciclo de vida do desenvolvimento de código;
    - ✓ Orientações no tratamento e remoção de vírus ou malware;
    - ✓ Liberação de acesso a navegação Web (filtro de conteúdo);
    - ✓ Qualquer outra requisição solicitada pela empresa relacionada à segurança da informação.

- Definir e documentar procedimentos de resposta e tratamento de incidentes de segurança da informação, para assegurar que todas as situações adversas sejam abordadas e tratadas de modo oportuno e eficiente;

- Cobrar e fiscalizar a revisão periódica de perfis de acesso pelos respectivos gestores e dono de processo;

- Promover aos novos Colaboradores treinamento para conscientização em Segurança da Informação com reciclagens periódicas.

6.5 Comitê de Segurança

O Comitê de Segurança deverá ser constituído por um gerente das áreas de: TI, Jurídico e Segurança da Informação, sendo as demais áreas convocadas mediante necessidade do tema.

Será responsabilidade do Comitê de Segurança:

- Receber os casos de violação desta política para encaminhamento às áreas pertinentes, alinhado com o Código de Ética do Grupo;

- Avaliar as situações envolvendo Segurança da Informação que eventualmente não estejam contempladas nesta Política;

- Definir os casos de aplicabilidade desta política e que ainda estejam em implementação pelos diversos projetos de Segurança;

- Receber e direcionar, conforme previsto na Política de Gestão de Riscos, casos que necessitem de assunção de riscos.

7. ANEXOS

Não aplicável.