POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

MENSAGEM DO PRESIDENTE

Para cumprirmos com nossa missão e garantir a fiel atuação dentro de nosso Código de Ética e Conduta apresentamos a nossa política de segurança da informação e comunicações.

Esperamos que cada colaborador dedique alguns minutos para reler e ponderar sobre o significado dessas regras no cumprimento de suas funções.

É de responsabilidade de todos o cumprimento destas regras, todos os dias, e em todas as situações em que forem aplicáveis.

Se você presenciar uma violação desta política deverá comunicá-la ao seu superior imediato ou ao representante do setor de Compliance da empresa, ou diretamente a nós.

Esperamos que vocês tenham o mesmo empenho que temos em colocar em prática a nossa missão e as orientações de nossas políticas.

_____

Presidente
Assinatura

Sumário

1. 1.PROPÓSITO 5
2. 2.OBJETIVO 6
3. 3.COMPETÊNCIAS E RESPONSABILIDADES 6
4. 4.DEFINIÇÕES 7
5. ATUALIZAÇÃO 7
6. 5.RESPONSABILIDADES DO USUÁRIO 7

5.1. REGRAS 7

5.1.1. Disposições gerais 7
5.1.2. Uso de recursos de TI 8
5.1.3. Uso de dispositivos portáteis 9
5.1.4. Uso da identificação e senhas de acesso 9
5.1.5. Política de mesa e tela limpa 10
5.1.6. Descarte de informações 10

7. 6.NORMA INSTITUCIONAL DE USO DA INTERNET 10

6.1. REGRAS 10

6.1.1. Disposições gerais 10
6.1.2. Redes sem fios 11
6.1.3. Permissão de acesso 11
6.1.4. Cancelamento e bloqueio do acesso à Internet 12
6.1.5. Uso da Internet 12
6.1.6. Monitoramento 13

8. 7.NORMA INSTITUCIONAL DE USO DO E-MAIL 14

7.1. REGRAS 14

7.1.1. Disposições iniciais 14
7.1.2. Permissão de acesso e criação de contas 14
7.1.4. Uso do correio eletrônico 15
7.1.5. Monitoramento 17

9. 8NORMA INSTITUCIONAL DE SEGURANÇA FÍSICA EM DATA CENTER 17

8.1. REGRAS 17

8.1.1. Disposições Gerais 17
8.1.2. Áreas de segurança do Data Center 18
8.1.3. Segurança ambiental 18

8.1.4. Instalação e proteção dos equipamentos 19
8.1.5. Controles de segurança do Data Center 19
10. 9.NORMA INSTITUCIONAL PARA CÓPIAS DE SEGURANÇA 21
9.1. REGRAS 21
9.1.1. Disposições Gerais 21
9.1.2. Cópias de segurança da informação 21
9.1.3. Armazenamento de mídias 22
9.1.4. Descarte / substituição de mídias 23
9.1.5. Restauração de cópias de segurança 23
11. 10. NORMA INSTITUCIONAL DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO E ATIVOS DE REDE 23
10.1. REGRAS 24
10.1.1. Disposições gerais 24
10.1.2. Requisitos de segurança de sistemas de informação 24
10.1.3. Processamento correto nas aplicações 24
10.1.4. Segurança dos arquivos do sistema 25
10.1.5. Segurança em processo de desenvolvimento e de suporte 25
10.1.6. Gestão de Vulnerabilidades técnicas 26
12. 11.NORMA INSTITUCIONAL DE ACESSO REMOTO 27
11.1. REGRAS 27
11.1.1. Disposições gerais 27
11.1.2. Do Acesso 27
11.1.3. Responsabilidades 28
13. 12. NORMA INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO CLASSIFICADA 28
12.1. REGRAS 28
12.1.1. Disposições gerais 28
12.1.2. Da proteção e do controle de informações sigilosas 29
12.1.3. Tratamento das Informações Pessoais 29
12.1.4. Dos sistemas de informação 30
12.1.5. Dos procedimentos para classificação de informação 31
12.1.6. Controles Criptográficos 31
14. 13.NORMA INSTITUCIONAL DE DISPOSITIVOS DO GRUPO FUSÃO 31
13.1. REGRAS 31

13.1.1. Disposições gerais 31
13.1.2. Uso dos dispositivos móveis corporativos 32
13.1.3. Considerações finais 32
15. 14. ..... GESTÃO DE CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES EM SEGURANÇA DA INFORMAÇÃO 33
14.1. Plano de Continuidade de Negócios – PCN 33
14.2. Identificação dos principais sistemas/ativos de TI 34
14.3. Análise de riscos, responsáveis e procedimentos de recuperação e contingência 34
16. 15.POLÍTICA DE PRIVACIDADE 41
15.1. Como coletamos os dados pessoais? 41
15.1.1. Identificadores eletrônicos (cookies) 41
15.1.2. Mídias Sociais 42
15.1.3. Dados pessoais transferidos por nossos parceiros comerciais 42
15.1.4. Dados de cadastro ou de contato 42
15.2. Quais dados pessoais são coletados, e para qual finalidade? 43
15.3. Com quem compartilhamos seus dados pessoais? 43
15.4. Exercício de seus direitos 44
15.6. Segurança dos Dados Armazenados 45
17. 16.OFICIAL DE PROTEÇÃO DE DADOS (DPO) 46
16.1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções: 46
16.2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. 46
18. 17.DISPOSIÇÕES FINAIS 47
19. 18.HISTÓRICO ..... **Erro! Indicador não definido.**

1. PROPÓSITO

Instituir a Política de Segurança da Informação do Grupo Fusão Soluções para Medicina a fim de assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações.

2. OBJETIVO

Estabelecer e difundir as Diretrizes da Política de Segurança da Informação no âmbito do Grupo Fusão, visando à orientação quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam, evitando impactos prejudiciais às atividades finais.

3. COMPETÊNCIAS E RESPONSABILIDADES

Instituir, no âmbito do Grupo Fusão, a seguinte estrutura para Gestão da Segurança da Informação e Comunicações:

I. O Gestor de Segurança da Informação;
II. O Comitê de Segurança da Informação, cuja composição será definida posteriormente;
III. Equipe de Tratamento de Incidentes de Rede, que funcionará em conformidade com norma específica.

São competências do Gestor de Segurança da Informação:

I. Promover cultura de segurança da informação;
II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III. Propor recursos necessários às ações de segurança da informação;
IV. Coordenar o Comitê de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
V. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI. Propor Normas e procedimentos relativos à segurança da informação no âmbito do Grupo Fusão.

São competências do Comitê de Segurança da Informação e Comunicações:

I. Assessorar na implementação das ações de segurança da informação e comunicações;
II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
III. Propor normas e procedimentos internos relativos à segurança da informação, em conformidade com as legislações existentes sobre o tema.

4. DEFINIÇÕES

Dado Pessoal: Informação relacionada a pessoa física identificada ou identificável. Um dado é considerado pessoal quando permite a identificação, direta ou indireta, da pessoa natural titular do dado, informações relacionadas a pessoa natural identificada ou identificável

Dado Pessoal Sensível: Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, são todos aqueles que podem causar discriminação a uma pessoa, merecendo maior proteção.

5. ATUALIZAÇÃO

A Política de Segurança da Informação será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

6. RESPONSABILIDADES DO USUÁRIO

Este documento dispõe sobre as responsabilidades do usuário quanto ao uso de senhas e equipamentos.

6.1. REGRAS

6.1.1. Disposições gerais

6.1.1.1. Todo usuário deve conhecer e cumprir a Política de Segurança da Informação e Comunicações.

6.1.1.2. O Grupo Fusão, através de sua área de comunicação, deve estabelecer um processo de divulgação permanente desta política, para a conscientização de todos os usuários.

6.1.2. Uso de recursos de TI

6.1.2.1. Os usuários devem proteger os recursos de TI contra acesso, modificação, destruição ou divulgação não autorizada.

6.1.2.2. Utilizar os recursos de TI colocados à sua disposição somente para os fins institucionais aos quais se destinam.

6.1.2.3. Não abrir o gabinete das estações de trabalho ou computador portátil, nem modificar qualquer configuração, seja de *hardware* ou *software*. Essas configurações são padronizadas, conforme definições da área de TI correlata. Havendo a necessidade de alteração destas configurações, a solicitação deve ser encaminhada à área de TI correlata para análise.

6.1.2.4. Não instalar ou executar *software* de sua propriedade ou de terceiros sem prévia homologação e autorização da área de TI correlata.

6.1.2.5. Desligar a estação de trabalho ou computador portátil corretamente e diariamente ao final do expediente, seguindo os procedimentos do sistema operacional.

6.1.2.6. As estações de trabalho ou computadores portáteis do Grupo Fusão devem ser ligadas somente em pontos elétricos estabilizados, evitando-se que sejam ligados em conjunto com outros equipamentos elétricos que não sejam recursos de TI.

6.1.2.7. Devem-se armazenar os arquivos com informações institucionais nos servidores de arquivos disponibilizados na rede local da Unidade. Deve-se evitar o armazenamento nas estações de trabalho.

6.1.2.8. Evitar realizar conversas em locais públicos ou sem a reserva adequada sobre assuntos sensíveis ao Grupo,

restringindo-se a tratá-los somente em locais que ofereçam a proteção adequada.

6.1.2.9. Colaborar ativamente na solução de problemas e no aprimoramento dos processos de segurança da informação.

6.1.3. Uso de dispositivos portáteis

6.1.3.1. Os dispositivos portáteis do Grupo Fusão, sempre que não estiverem sendo utilizados, devem ser guardados em local seguro, onde o responsável, por estes, possa garantir que os mesmos não serão utilizados por outras pessoas.

6.1.3.2. O uso de dispositivos portáteis pessoais deve ser avaliado pela área de TI correlata.

6.1.4. Uso da identificação e senhas de acesso

6.1.4.1. O Usuá rio somente terá acesso às informações e aos recursos de TI após a conclusão do processo de credenciamento/concessão de acesso, que se dará através de solicitação formal da chefia imediata do usuário à área de Recursos Humanos da Unidade, que por sua vez fará o encaminhamento à área de TI correlata. Deve ser seguido a regra de mínimo acesso necessário para o usuário.

6.1.4.2. Da mesma forma a modificação, revisão, desabilitação e remoção do acesso se dará através de solicitação formal da chefia imediata do usuário à área de Recursos Humanos da Unidade, que por sua vez fará o encaminhamento à área de TI correlata.

6.1.4.3. A cada usuário deve ser disponibilizada apenas uma identificação de acesso aos recursos de TI. Essa identificação deve ser única, pessoal e intransferível.

6.1.4.4. A senha de acesso ao recurso de TI qualifica o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela área de TI correlata.

6.1.4.5. Os direitos e perfis de acesso seguem as definições do responsável pelo usuário em concordância com os padrões estabelecidos pela área de TI correlata.

6.1.4.6. O usuário não deve compartilhar sua senha de acesso com outras pessoas.

6.1.4.7. Onde tecnicamente possível, a senha deve ter ao menos 8 caracteres

6.1.4.8. Onde tecnicamente possível, as senhas devem exigir uma combinação de letras, números e caracteres especiais (para complexidade)

6.1.4.9. O usuário deve trocar sua senha de acesso aos recursos de TI periodicamente, seguindo as orientações da área de TI correlata. Quando não definida regra específica a senha deve ser alterada em no máximo noventa dias.

6.1.5. Política de mesa e tela limpa

6.1.5.1. Os documentos impressos devem ser classificados em conformidade com a legislação vigente.

6.1.5.2. Os documentos sigilosos não devem ser deixados sobre as mesas na ausência do usuário e devem ser guardados em local seguro e com controle de acesso.

6.1.5.3. Bloquear o acesso à estação de trabalho ou computador portátil que lhe foi confiado sempre que dele se ausentar.

6.1.6. Descarte de informações

6.1.6.1. Os ativos não mais utilizados pelos usuários, em meio eletrônico ou não, devem ser apagados ou destruídos conforme regras da legislação vigente.

7. NORMA INSTITUCIONAL DE USO DA INTERNET

Este documento dispõe sobre as regras de segurança relativas ao uso do serviço da Internet.

7.1. REGRAS

7.1.1. Disposições gerais

7.1.1.1. O acesso à Internet disponibilizado aos usuários de rede pelo Grupo Fusão deve ser realizado somente para os interesses de negócio da Instituição.

7.1.1.2. O Grupo Fusão permite o uso parcimonioso da Internet para interesses particulares dos usuários da rede, desde que este uso não exceda os limites da ética, bom senso e razoabilidade, bem como não contenha, receba ou transmita informações institucionais.

7.1.1.3. É atribuição exclusiva da área de TI correlata definir os softwares para uso da Internet na Unidade.

7.1.1.4. O uso dos recursos computacionais do Grupo Fusão para acesso à Internet nas instalações do grupo, somente será permitido quando realizado através de redes de dados homologadas pelas áreas de TI correlatas.

7.1.1.5. O acesso à Internet por meio da rede local não pode ser realizado se utilizando mais de um meio de comunicação simultaneamente.

7.1.1.6. O acesso à Internet por meio da rede local não pode ser realizado por equipamentos particulares, tais como laptops, smartphones, etc. Casos excepcionais devem ser tratados pela área de TI correlata.

7.1.2. Redes sem fios

7.1.2.1. Os usuários do Grupo Fusão podem acessar a rede sem fios da Unidade através de seus usuários e senhas corporativos (WPA2 – Enterprise)

7.1.2.2. Os visitantes devem solicitar usuário e senha ao administrativo da Unidade e logar através de Portal Captivo. Este usuário é válido por 4 horas.

7.1.2.3. Os visitantes precisam aceitar a política de uso no Portal Captivo antes de obter acesso à rede.

7.1.3. Permissão de acesso

7.1.3.1. A todo usuário da rede local do Grupo Fusão é facultado o acesso a Internet em conformidade com os termos estabelecidos nesta norma.

7.1.4. Cancelamento e bloqueio do acesso à Internet

7.1.4.1. O acesso à Internet pelo usuário da rede será obrigatoriamente desativado quando ocorrer o desligamento do usuário.

7.1.5. Uso da Internet

7.1.5.1. O acesso à Internet concedido ao usuário de rede do Grupo Fusão é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos causados por meio de seu uso.

7.1.5.2. O uso da Internet através da rede corporativa não poderá ser feito via *proxies* externos.

7.1.5.3. O usuário da rede deverá utilizar a Internet de forma a não causar tráfego desnecessário na rede corporativa.

7.1.5.4. Todo serviço disponibilizado na Internet, antes de ser implantado na rede corporativa, deve ser avaliado pela área de TI correlata através de avaliação e relatório técnico, considerando os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

7.1.5.5. É vedada a utilização da Internet para:

- Acessar sites com códigos maliciosos;
- Acessar sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;
- Acessar sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;
- Acessar sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;

- Realizar download de arquivos que não estejam relacionados às necessidades de trabalho;
- Realizar atividades relacionadas a jogos eletrônicos pela Internet;
- Escutar música ou assistir programas de TV, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho;
- Acessar sites para transferência de arquivos, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho;
- Utilizar serviços de compartilhamento de arquivos online, salvo aqueles homologados pela área de TI correlata.

7.1.5.6. O usuário deve sempre se certificar da procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no navegador.

7.1.5.7. É vedado aos usuários disponibilizar informações de propriedade do Grupo Fusão em sites da Internet sem observar sua classificação e o público a que se destina.

7.1.5.8. A utilização de equipamentos pessoais no ambiente do Grupo Fusão não poderá ser realizada por meio da rede corporativa, salvo quando a Unidade dispuser de uma rede isolada específica para este fim e mediante a concordância do termo de responsabilidade pelo usuário.

7.1.6. Monitoramento

7.1.6.1. O acesso à Internet é monitorado e pode ser restringido pela área de TI correlata quanto a endereço de sites, quantidade de acessos, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que estes controles sejam feitos por parâmetros gerais.

7.1.6.2. A área de recursos humanos ou chefias hierarquicamente superiores podem solicitar formalmente um relatório com as informações de acesso à Internet de um de

seus usuários da rede, para si ou para outros, nas seguintes situações:

- Suspeita de infração à Política de Segurança da Informação e Comunicações;
- Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus usuários de rede.

8. NORMA INSTITUCIONAL DE USO DO E-MAIL

Este documento dispõe sobre as regras de segurança relativas ao uso do serviço de correio eletrônico.

8.1. REGRAS

8.1.1. Disposições iniciais

8.1.1.1. A conta de correio eletrônico institucional, disponibilizada aos usuários da rede de dados do Grupo Fusão, deve ser utilizada somente para os interesses de trabalho.

8.1.1.2. A conta de correio eletrônico institucional disponibilizada ao usuário da rede de dados do Grupo Fusão é pessoal e intransferível, sendo seu titular o único e total responsável pelo seu uso e suas consequências.

8.1.1.3. É atribuição exclusiva da área de TI correlata definir os softwares homologados para o uso do correio eletrônico institucional.

8.1.1.4. É atribuição exclusiva da área de TI correlata normatizar o uso do correio eletrônico particular.

8.1.1.5. Quando a área de TI correlata permitir o uso do correio particular, o usuário não deverá exceder os limites da ética, bom senso e razoabilidade, sendo o responsável pelo conteúdo trafegado e seus eventuais riscos.

8.1.1.6. É proibido o uso de provedores de e-mail externos para o encaminhamento das mensagens de uma caixa postal do Grupo Fusão.

8.1.2. Permissão de acesso e criação de contas

8.1.2.1. O usuário terá direito a uma única conta de e-mail que o identificará univocamente em todo Grupo Fusão.

8.1.2.2. A conta de correio eletrônico institucional deve ser revalidada anualmente. A não revalidação implicará no cancelamento da conta.

8.1.2.3. A caixa postal compartilhada ou lista de discussão deve ter um responsável e um substituto formalizados.

8.1.3. Cancelamento, bloqueio, suspensão ou desbloqueio do correio eletrônico.

8.1.3.1. Cabe à área de Recursos Humanos de cada unidade comunicar à área de TI correlata o cancelamento, bloqueio, suspensão ou desbloqueio da conta de correio do usuário.

8.1.3.2. O do correio eletrônico institucional é uma concessão do Grupo Fusão e será desativado:

8.1.3.3. No caso de afastamento do usuário, o acesso à sua caixa de correio eletrônico respeitará as normas estipuladas pela Diretoria de Recursos Humanos.

8.1.4. Uso do correio eletrônico

8.1.4.1. As caixas postais do correio eletrônico institucional possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo da área de TI provedora do serviço definir esses limites.

8.1.4.2. Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido pela área de TI provedora do serviço.

8.1.4.3. É vedada a utilização do correio eletrônico institucional para:

- Realizar Spam;
- Contribuir com a continuidade de correntes de mensagens eletrônicas;
- Utilizá-lo com objetivos político-partidários, religiosos, entre outros;
- Receber de forma consentida, armazenar ou enviar mensagens com:

- Vírus de computador, cavalo de Tróia, Spyware e outros códigos maliciosos;
- Material pornográfico, atentatório à moral e aos bons costumes ou ofensivos;
- Conteúdo criminoso, ilegal, ou que façam sua apologia;
- Conteúdo discriminatório (racial, religioso, etc.) ou de incitação à violência;
- Conteúdo que desrespeitem os direitos autorais.

8.1.4.4. De forma a preservar o funcionamento do serviço de correio eletrônico institucional, o Usuário da rede de dados deve:

- Eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa postal;
- Evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de softwares maliciosos ou direcionar o usuário da rede de dados para um site falso, possibilitando a captura de informações;
- Evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência. No caso de suspeita de irregularidade na mensagem, o usuário deve solicitar ajuda a área de TI correlata;

8.1.4.5. Todo usuário da rede de dados do Grupo Fusão, antes de enviar mensagens pelo correio eletrônico institucional, deve levar em conta a classificação da informação, conforme legislação vigente.

8.1.4.6. O uso da conta de correio eletrônico institucional em listas de discussão ou distribuição deve se limitar aos casos de necessidade do trabalho ou atividade desempenhada.

8.1.4.7. O correio eletrônico particular não deve ser utilizado para o envio ou recebimento de informações do Grupo Fusão.

8.1.4.8. O correio eletrônico institucional não deve ser utilizado para fim particular, como cadastro de comércio eletrônico, por exemplo.

8.1.4.9. O Grupo Fusão não se responsabiliza em fornecer suporte técnico ao correio eletrônico particular.

8.1.5. Monitoramento

8.1.5.1. O correio eletrônico institucional pode ser monitorado e restringido pela área de TI correlata, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).

8.1.5.2. Nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações, a área de TI correlata poderá acessar a caixa postal institucional do respectivo usuário através de ato administrativo ou judicial;

9. NORMA INSTITUCIONAL DE SEGURANÇA FÍSICA EM DATA CENTER

Este documento dispõe sobre as regras para prevenção de acesso não autorizado, dano ou interferência às informações, recursos tecnológicos e instalações físicas em Data Centers do Grupo Fusão.

9.1. REGRAS

9.1.1. Disposições Gerais

9.1.1.1. O acesso ao Data Center é permitido aos agentes credenciados e portadores da identificação física.

9.1.1.2. A identificação física dos agentes lotados no Data Center deve ser distinta dos demais;

9.1.1.3. Os agentes devem utilizar a identificação física em local de fácil visualização;

9.1.1.4. Os agentes devem comunicar imediatamente a perda, furto ou desaparecimento da sua identificação física à área de segurança da informação;

9.1.2. Á reas de segurança do Data Center

9.1.2.1. Todas as instalações de processamento ou armazenamento de informações sensíveis devem ser mantidas em áreas de segurança do Data Center;

9.1.2.2. As permissões de acesso físico às áreas de segurança do Data Center devem ser mensalmente revisadas.

9.1.2.3. As á reas de segurança do Data Center devem ser claramente definidas com a utilização de barreiras de segurança e mecanismos de controle de acesso, de forma a impedir o acesso não autorizado;

9.1.2.4. Deve ser evitada a utilização de informações visuais que identifiquem as áreas de atividade de processamento e guarda das informações;

9.1.3. Segurança ambiental

9.1.3.1. O Data Center deve estar posicionado em local seguro, protegido por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso de acordo com criticidade associada aos seus ativos e informações;

9.1.3.2. A edificação do Data Center deve ser protegida contra descargas elétricas atmosféricas;

9.1.3.3. As portas e janelas do Data Center devem ser mantidas fechadas;

9.1.3.4. Suprimentos e materiais de escritório não devem ser armazenados em áreas de segurança, a menos que requeridos;

9.1.3.5. Equipamentos de contingência e mídias com cópias de segurança devem ser armazenados a uma distância segura da instalação principal;

9.1.3.6. Todo trabalho realizado por terceiros no Data Center deve ser registrado e supervisionado;

9.1.3.7. As instalações elétricas, de cabeamento lógico e dos equipamentos de detecção e combate a incêndio devem ser feitas de acordo com o especificado nas normas da ABNT;

9.1.3.8. É proibido o manuseio de alimentos, bebidas e cigarros, bem como o consumo no Data Center.

9.1.4. Instalação e proteção dos equipamentos

9.1.4.1. É proibida a ligação de mais de um equipamento em uma mesma tomada;

9.1.4.2. Os equipamentos de TI do Data Center devem ser instalados em *racks*, sempre que possível;

9.1.4.3. Os equipamentos cuja dimensão impeça a instalação dentro de racks devem ter seus botões de ligar/desligar devidamente protegidos contra acessos ou internamente desconectados, de forma a evitar seu acionamento local;

9.1.4.4. As chaves dos *racks* e dos quadros de força devem receber identificação e serem guardadas em um claviculário em local adequado, protegido contra acesso indevido;

9.1.4.5. Deve ser designado um responsável pela chave do claviculário, que deverá registrar todas as retiradas e devoluções de chaves;

9.1.4.6. A identificação adotada deve ser de difícil dedução para pessoas estranhas ao ambiente;

9.1.5. Controles de segurança do Data Center

9.1.5.1. Os acessos ao Data Center devem ser monitorados por circuito fechado de TV (CFTV). Câmeras de monitoramento devem ser instaladas em locais estratégicos do ambiente, seja ele interno ou externo.

9.1.5.2. As imagens captadas pelas câmeras do circuito interno de TV devem ser gravadas de forma contínua, visando embasar

futuras investigações em caso de suspeitas ou incidentes de segurança.

9.1.5.3. Os arquivos das imagens gravadas devem ser guardados pelo período mínimo de um ano, sendo tratados com os mesmos critérios das mídias de cópia de segurança.

9.1.5.4. As imagens gravadas pelo circuito interno de TV devem ser periodicamente analisadas, a fim de identificar possíveis eventos que contrariem a Política de Segurança.

9.1.5.5. O sistema de circuito fechado de TV deve ser monitorado, alertando a equipe em caso de indisponibilidade no funcionamento.

9.1.5.6. As portas de acesso ao Data Center devem possuir mecanismos de fechamento automático.

9.1.5.7. Alarmes de intrusão devem ser instalados nas portas e janelas do Data Center.

9.1.5.8. As portas de acesso devem possuir dispositivo de controle de acesso, tais como crachá por aproximação e solicitação de senha.

9.1.5.9. A entrada no Data Center deve ser condicionada somente as pessoas autorizadas pela área de T.I.

9.1.5.10. Apó s o horário normal de trabalho, o acesso para qualquer pessoa que não esteja envolvida na administração, gerenciamento ou operação do Data Center, será permitido somente através de autorização emitida pela chefia área de TI correlata.

9.1.5.11. É de responsabilidade dos agentes lotados no Data Center, registrar e acompanhar os prestadores de serviço e visitantes, sendo responsáveis pelas ações destes enquanto permanecerem no ambiente.

9.1.5.12. A coleta de lixo e limpeza do Data Center deve ser realizada por pessoas instruídas quanto os cuidados necessários para tal serviço, devendo sempre ser autorizadas,

registradas e acompanhadas por agente público lotado no ambiente.

9.1.5.13. Devem-se definir os dias e horários destinados à limpeza do Data Center, de forma a não comprometer a prestação dos serviços disponibilizados pela área.

9.1.5.14. A entrada e saída de qualquer ativo devem ser registradas.

9.1.5.15. É proibida a entrada de equipamentos de fotografia, vídeo e áudio.

9.1.5.16. Os ramais telefônicos devem ser restritos a chamadas internas.

9.1.5.17. Somente pessoas autorizadas podem portar equipamentos eletrônicos portáteis (celular, pen drive, palms, etc.) no interior do Data Center.

10. NORMA INSTITUCIONAL PARA CÓPIAS DE SEGURANÇA

Este documento estabelece as diretrizes para a geração de cópias de segurança das informações e sua recuperação em um tempo aceitável.

10.1. REGRAS

10.1.1. Disposições Gerais

10.1.1.1. Convém que as cópias de segurança das informações e de *software* sejam efetuadas e testadas regularmente pela área de TI correlata.

10.1.1.2. Convém que a infraestrutura para a geração de cópias de segurança seja adequada para garantir que toda informação essencial possa ser recuperada.

10.1.1.3. Convém que informações sensíveis sejam salvaguardadas criptografadas nas cópias de segurança.

10.1.2. Cópias de segurança da informação

10.1.2.1. A área de TI correlata é a responsável pelo processo de cópias de segurança no âmbito das Unidades do Grupo Fusão.

10.1.2.2. Os equipamentos envolvidos no processo de cópias de segurança devem garantir que os dados selecionados sejam gravados na sua totalidade.

10.1.2.3. As cópias de segurança devem ser realizadas em horário de baixa utilização das informações, preferencialmente fora do horário de expediente.

10.1.2.4. Sendo inevitável a realização de cópias de segurança no horário do expediente deverá ser justificado antecipadamente caso haja necessidade de parada do serviço ou queda no desempenho dos recursos de TI.

10.1.2.5. Cada área de TI correlata deve definir e regulamentar os critérios necessários das cópias de segurança, a frequência, a extensão (completa, diferencial e incremental) e o seu período de retenção.

10.1.2.6. Cabe à área de TI correlata definir procedimentos para a geração e restauração das cópias de segurança, mantendo os registros completos e fidedignos das cópias de segurança.

10.1.2.7. Deve ser implementado um controle de acesso físico e lógico para as informações das cópias de segurança.

10.1.2.8. As cópias de segurança devem ser testadas regularmente e os registros das evidências dos testes devem ser devidamente documentados.

10.1.2.9. Os mecanismos de cópias de segurança devem ser automatizados, a fim de facilitar os processos de geração e recuperação.

10.1.3. Armazenamento de mídias

10.1.3.1. As mídias devem ser armazenadas em local distinto da área de TI correlata, a uma distância suficiente para preservá-las de possíveis ameaças, respeitando as recomendações dos fabricantes.

10.1.3.2. As mídias devem ser armazenadas em local seguro com acesso restrito e controlado somente a usuários autorizados.

10.1.3.3. As mí dias devem ser devidamente identificadas de forma a permitir sua rápida localização e recuperação.

10.1.3.4. As mí dias devem ser transportadas por um colaborador autorizado pela área de TI correlata, para um local seguro, dentro de embalagem lacrada que proteja adequadamente o seu conteúdo.

10.1.4. Descarte / substituição de mídias

10.1.4.1. Para cada tipo de mídia devem ser observados os critérios do fabricante quanto aos seus requisitos de utilização.

10.1.4.2. No caso de mudança de infraestrutura tecnológica, as mídias com informações que ainda não expiraram devem ser transferidas para as novas mídias.

10.1.4.3. Devem-se adotar mecanismos seguros para o descarte de mídias (incineração, trituração, etc.) a fim de garantir que informações armazenadas e sem uso sejam irrecuperáveis, observando as legislações pertinentes.

10.1.4.4. Mí dias a serem descartadas devem ser registradas e suas informações de identificação devem ser removidas.

10.1.5. Restauração de cópias de segurança

10.1.5.1. A á rea de TI correlata deve realizar regularmente testes de restauração das cópias de segurança em ambiente distinto ao de produção e suas evidências dos testes devem ser devidamente documentados.

10.1.5.2. O usuá rio deve solicitar formalmente a restauração de uma cópia de segurança, de acordo com procedimento definido pela área de TI correlata.

11. NORMA INSTITUCIONAL DE AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO E ATIVOS DE REDE

Este documento estabelece as diretrizes de segurança para aquisição, desenvolvimento e manutenção de sistemas da informação no âmbito do Grupo Fusão.

11.1. REGRAS

11.1.1. Disposições gerais

11.1.1.1. Todos os requisitos de segurança devem ser identificados e justificados na fase de definição de requisitos de um projeto, acordados e documentados.

11.1.1.2. Todo projeto de sistema de informação antes da sua concepção, inclusive aquele desenvolvido pelo usuário, deve ser submetido à área de TI correlata para avaliação/homologação dos aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

11.1.1.3. Os sistemas de informação classificados como críticos deverão ser desenvolvidos levando em consideração requisitos para sua contingência.

11.1.1.4. Todos os usuários que utilizarão um sistema devem ser treinados e capacitados para exercer suas atividades.

11.1.2. Requisitos de segurança de sistemas de informação

11.1.2.1. Devem ser considerados requisitos de segurança na definição dos novos sistemas.

11.1.2.2. Devem ser considerados requisitos de segurança na aquisição de novos sistemas.

11.1.2.3. Devem ser considerados requisitos de segurança em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

11.1.3. Processamento correto nas aplicações

11.1.3.1. Devem ser incorporados controles apropriados em projetos de aplicações para assegurar o processamento correto.

11.1.3.2. Os controles devem incluir os dados de entrada, o processamento interno e os dados de saída.

11.1.3.3. Controles adicionais para sistemas que processem informações sensíveis, valiosas ou críticas ou que nessas

exerçam algum impacto devem ser determinados com base em requisitos de segurança e análise/avaliação de riscos.

11.1.3.4. Os dados de entrada de aplicações devem ser validados para garantir que são corretos e apropriados.

11.1.3.5. Devem ser incorporadas nas aplicações checagens de validação com o objetivo de detectar qualquer corrupção de informações por erros ou por ações deliberadas.

11.1.3.6. Devem ser identificados e implementados requisitos e controles apropriados para garantir a autenticidade e proteger a integridade das mensagens em aplicações.

11.1.3.7. Devem ser validados os dados de saída das aplicações para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias.

11.1.3.8. A utilização dos recursos e as projeções feitas para a necessidade de capacidade futura devem ser monitoradas de modo a garantir o desempenho requerido do sistema de informação.

11.1.4. Segurança dos arquivos do sistema

11.1.4.1. Devem ser documentados os procedimentos para a instalação e atualização de softwares.

11.1.4.2. A massa de dados utilizados nos testes da fábrica de software deve ser diferente da utilizada no ambiente de produção.

11.1.4.3. O acesso aos códigos fontes dos sistemas deve ser controlado e autorizado pela área de TI correlata.

11.1.5. Segurança em processo de desenvolvimento e de suporte

11.1.5.1. Deve ser documentado e implementado um processo de gestão de mudanças.

11.1.5.2. A á rea de TI correlata deve supervisionar o processo desde o seu planejamento até a implementação no caso de desenvolvimento de softwares por terceiros.

11.1.5.3. Deve ser implementado controle de versão para garantir a gestão dos códigos fontes.

11.1.5.4. Deve ser realizada a análises de riscos a fim de detectar falhas nos sistema que possam comprometer a segurança da informação.

11.1.5.5. O suporte dos sistemas somente poderá ser realizado após abertura de chamado (para registro dos eventos).

11.1.5.6. Devem ser protegidas as informações envolvidas em transações *online*, a fim de prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

11.1.6. Gestã o de Vulnerabilidades técnicas

11.1.6.1. Devem ser investigado e tratado de forma contínua as vulnerabilidades técnicas dos sistemas de informação em uso.

11.1.6.2. Devem ser avaliada e implementada medidas apropriadas para lidar com os riscos associados a uma eventual vulnerabilidade.

11.1.6.3. A equipe de TI faz análises de avaliação de riscos e vulnerabilidades proativamente. Baseado nestas análises faz um plano de ação para a remediação dos riscos e vulnerabilidades encontrados e em caso de incorrência de custos para implementação deve ser apresentada ao comitê de segurança para aprovação.

11.1.6.4. Gestão de Patches e atualizações dos sistemas:

11.1.6.4.1. A equipe de TI correlata deve monitorar as soluções dos fabricantes de softwares e hardware quanto a atualizações corretivas.

11.1.6.4.2. A cada atualização disponível a equipe de TI avalia a criticidade das vulnerabilidades a serem corrigidas e define o calendário de implementação do mesmo. Este calendário deve variar com o impacto no negócio, sendo

que vulnerabilidades de alto risco em sistema operacional de usuário deve ser analisado e executado em no máximo 2 dias e em sistema operacional de servidores ou sistemas de negócio deve ser avaliado por no mínimo 5 dias antes de sua implementação em produção.

11.1.6.4.3. A implementação das atualizações deve ser realizada em ambiente de testes para a homologação antes de sua implementação definitiva.

12. NORMA INSTITUCIONAL DE ACESSO REMOTO

Este documento estabelece as diretrizes para a realização de acesso à rede de dados do Grupo Fusão a partir de um local externo.

12.1. REGRAS

12.1.1. Disposições gerais

12.1.1.1. O acesso remoto a uma rede de dados do Grupo Fusão será de acordo com as necessidades, somente para fins de trabalho.

12.1.1.2. Deve ser formalizado junto à área de TI correlata o pedido de acesso remoto, justificando a necessidade de acesso e período de uso.

12.1.1.3. A á rea de TI correlata deve registrar o acesso remoto do usuário.

12.1.1.4. O acesso remoto deve ser concedido por um período de tempo pré-definido.

12.1.2. Do Acesso

12.1.2.1. O acesso remoto a uma rede de dados do Grupo Fusão deve ser realizado por meio de canal criptografado e solicitação de autenticação do Usuário utilizando ferramentas de autenticação por múltiplos fatores.

12.1.2.2. A á rea de TI correlata deve informar aos usuários os requisitos mínimos de segurança estabelecidos para realização de acesso remoto.

12.1.2.3. Os recursos de Tecnologia da Informação – TI utilizados no ambiente de trabalho remoto, tal como residências, devem conter mecanismos de proteção contra vírus, software malicioso e controle de acesso.

12.1.2.4. O acesso a uma rede de dados do Grupo Fusão deve ser permitido somente a partir de recursos de TI que foram previamente cadastrados e homologados pela área de TI correlata.

12.1.2.5. Quando os recursos de informática forem de propriedade de terceiros, a área de TI correlata deve solicitar a estes que os referidos recursos atendam aos requisitos mínimos de segurança estipulados.

12.1.2.6. A á rea de TI correlata deve garantir aos Usuários que fazem uso do acesso remoto a uma rede de dados a capacitação quanto à utilização da solução de acesso.

12.1.3. Responsabilidades

12.1.3.1. A á rea de TI correlata deve prover mecanismos de proteção adequados às redes de dados sob responsabilidade de sua Unidade, bem como aos serviços a elas conectados.

12.1.3.2. O usuá rio é responsável por toda e qualquer operação (acesso, processamento, comunicação, etc.) realizada através de um acesso remoto.

13. NORMA INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

Este documento estabelece as diretrizes para classificação e tratamento das informações quanto ao seu grau de sigilo nos aspectos referentes à segurança da informação e comunicações.

13.1. REGRAS

13.1.1. Disposições gerais

13.1.1.1. Deve-se classificar a informação em termos de seu valor, requisitos legais, sensibilidade e criticidade.

13.1.1.2. O nível de proteção deve ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação.

13.1.1.3. Os procedimentos de rotulação da informação precisam abranger tanto os ativos de informação no formato eletrônico quanto no formato físico.

13.1.2. Da proteção e do controle de informações sigilosas

13.1.2.1. É dever do grupo Fusão assegurar a proteção e controlar o acesso e a divulgação de informações sigilosas produzidas por suas unidades.

13.1.2.2. Entidades públicas ou privadas que tiverem algum vínculo com o Grupo Fusão para o tratamento ou o uso de informações sigilosas deverão observar as regulamentações das leis vigentes, inclusive instruir seus empregados, prepostos ou representantes a observarem as medidas e procedimentos de segurança das informações classificadas quanto ao seu grau de sigilo.

13.1.2.3. Aquele que tiver acesso à informação classificada cria a obrigação de resguardar o sigilo.

13.1.2.4. O acesso, a divulgação e o tratamento de informações classificadas como sigilosas ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma das regulamentações das leis vigentes.

13.1.3. Tratamento das Informações Pessoais

13.1.3.1. O tratamento das informações pessoais deve respeitar à intimidade, a honra, a vida privada e a imagem das pessoas.

13.1.3.2. Terceiros poderão ter acessos às informações pessoais mediante previsão legal ou consentimento expresso da pessoa a que se refere às informações.

13.1.4. Dos sistemas de informação

13.1.4.1. Devem ser utilizados sistemas de informação e canais de comunicação seguros.

13.1.4.2. As informações, classificadas em qualquer grau de sigilo, contidas em sistemas de informação, devem ser transmitidas através da rede corporativa por meio de um canal seguro.

13.1.4.3. De forma a garantir a autenticidade, a identidade do usuário da rede deve ser garantida minimamente pelo uso de autenticação individual e utilizando Autenticação Multifator (MFA).

13.1.4.4. Os sistemas de informação devem prever níveis de controle de acesso e recursos criptográficos adequados aos graus de sigilo. Todos os arquivos de interesse do Grupo devem ser armazenados apenas na plataforma de nuvem criptografada (Sharepoint).

13.1.4.5. Os sistemas de informação devem manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por um prazo igual ou superior ao de restrição da informação.

13.1.4.6. Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar ligados a canais de comunicação seguros, que estejam fisicamente ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

13.1.4.7. Toda a informação, classificada em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deve ser protegida com recurso criptográfico.

13.1.4.8. Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais para sua criação, controle para o seu acesso, manutenção, armazenamento,

transferência, trânsito e descarte, em conformidade com a legislação vigente.

13.1.5. Dos procedimentos para classificação de informação

13.1.5.1. Os documentos com dados classificados devem conter as seguintes informações: código de indexação do documento, grau de sigilo, categoria na qual se enquadra a informação, tipo de documento, data da produção do documento, indicação de dispositivo legal que fundamenta a classificação, razões da classificação, indicação do prazo de sigilo e data da classificação.

13.1.6. Controles Criptográficos

13.1.6.1. Todos os dispositivos do Grupo Fusão devem possuir a função de Bitlocker habilitada.

13.1.6.2. Todos os arquivos de interesse do Grupo devem ser armazenados apenas na plataforma de nuvem criptografada Sharepoint Online e todos os acessos à mesma devem utilizar autenticação de múltiplos fatores.

13.1.6.3. Todos os sistemas de informação utilizados no grupo devem ser baseados em nuvem segura, Oracle Cloud Infrastructure, e seu acesso pelo usuário deverá ser realizado através de ferramenta TSPLUS também garantindo a criptografia dos dados em trânsito.

14. NORMA INSTITUCIONAL DE DISPOSITIVOS DO GRUPO FUSÃO

14.1. REGRAS

14.1.1. Disposições gerais

14.1.1.1. O uso de dispositivos móveis no Grupo Fusão deve ser pautado na necessidade e interesse da empresa;

14.1.1.2. O usuário deve ser orientado a respeito dos procedimentos de segurança e a responsabilidade que o mesmo passa a assumir acerca do uso dos dispositivos móveis, mediante assinatura de um termo de uso e responsabilidade,

não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido;

14.1.1.3. Os dispositivos móveis devem ser utilizados somente pelos usuários que assumiram formalmente a responsabilidade pelo seu uso;

14.1.2. Uso dos dispositivos móveis corporativos

14.1.2.1. Os dispositivos móveis corporativos devem ser inventariados através de instalação de cliente específico pela equipe de TI;

14.1.2.2. Os dispositivos móveis devem possuir somente os softwares homologados e instalados pela área de TI correlata;

14.1.2.3. O Usuá rio não deve instalar ou desinstalar qualquer tipo de software nos dispositivos;

14.1.2.4. Os dispositivos devem ser registrados como membros de um domínio de rede;

14.1.2.5. Os dispositivos devem oferecer mecanismos que garantam o controle de acesso e sigilo das informações neles armazenada. (Exemplo: senhas, usuários, tokens, criptografia dos dados, biometrias e etc.)

14.1.2.6. É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e/ou dispositivo, às conexões de rede e recursos disponíveis;

14.1.2.7. A á rea de TI correlata deve adotar mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio;

14.1.3. Considerações finais

14.1.3.1. O Usuário deve bloquear seu dispositivo móvel ao se afastar do mesmo, evitando que outras pessoas tenham acesso às informações armazenadas;

14.1.3.2. No caso de equipamentos que não são de uso contínuo, quando fora de uso, devem ser desligados e guardados em local que somente o seu responsável tenha acesso;

14.1.3.3. O usuá rio deve realizar uma varredura com o software antivírus disponível antes de gravar no equipamento portátil de TI qualquer informação que receba por e-mail ou mídias de armazenamento removíveis;

14.1.3.4. O usuá rio deve proteger o equipamento de TI e os dados nele contidos contra situações de risco. Tais proteções incluem: não deixá-lo sozinho, não permitir que outra pessoa tenha acesso às informações nele armazenadas, etc.

14.1.3.5. O Usuá rio deve providenciar a transferência das informações institucionais manipuladas no equipamento de TI para os servidores de rede do Grupo Fusão;

14.1.3.6. A á rea de TI correlata não se responsabilizará por informações armazenadas nos dispositivos móveis;

14.1.3.7. As unidades devem observar os requisitos de segurança descritos nesta norma ao adquirir dispositivos móveis corporativos, independentemente de serem consignados ou não.

15. GESTÃO DE CONTINUIDADE DE NEGÓCIOS E RECUPERAÇÃO DE DESASTRES EM SEGURANÇA DA INFORMAÇÃO

A finalidade desta Política é definir o escopo e as regras básicas de gestão de continuidade dos negócios.

15.1. Plano de Continuidade de Negócios – PCN

O PCN é um documento que visa realizar o planejamento das ações que devem ser executadas em uma situação de crise que afete as operações de negócio. Ele possibilita a à organização continuar suas atividades em um nível aceitável pré-definido.

Esse plano é, na verdade, constituído de 3 documentos:

- Plano de administração de crise: é um documento disponibilizado para a alta gestão que objetiva dá mais controle para organização em caso de uma situação de crise. Contém informações como: listas de contatos e relação de atividades das equipes envolvidas.

- Plano de continuidade operacional: documento onde são definidos os procedimentos de resposta para estabilizar a situação na ocorrência de um incidente ou evento indesejado. Seu principal objetivo é identificar principais tipos de incidentes, checar a existência de procedimentos de respostas apropriados e criar procedimentos novos de contingência que ainda não existem. As etapas desse plano são: realizar uma análise do ambiente, elaborando as hipóteses e os possíveis cenários de crise; definir objetivos e metas, analisando a viabilidade e a prioridade com que os danos serão tratados; organizar a equipe, elaborando a estrutura organizacional que vai dar suporte ao plano, definindo procedimentos para ativação do plano, níveis de autoridade, papéis e as responsabilidades.
- Plano de recuperação de desastre - define os procedimentos para restaurar, no menor tempo possível, as operações de tecnologia da informação em caso de interrupção não-programada. Também devem prever os impactos da paralisação e o tempo máximo necessário para a recuperação as atividades essenciais da organização.

15.2. Identificação dos principais sistemas/ativos de TI

Além de sistemas que apoiam diretamente os processos de negócio, alguns ativos de TI foram incluídos nessa lista, devido a relevância desses ativos para o funcionamento de todos os sistemas.

- Sistema Visto
- Link de internet
- Servidor de arquivos corporativos.
- E-mail
- Sistema de autenticação de usuários (AD)

15.3. Análise de riscos, responsáveis e procedimentos de recuperação e contingência

Sistema/Ativo	Impacto no negócio
Sistema Visto	Alto
Link de Internet	Alto
Servidor de arquivos corporativos	Alto
E-mail	Médio

Sistema de Autenticação de usuários	Baixo

15.3.1. Sistema Visto

Sistema localizado em estrutura de nuvem da Oracle (Oracle Cloud Infrastructure)

Risco e Probabilidade	Responsável da Fusão	Ação de Contingência	Tempo de Recuperação
Falha de Hardware (baixa)	PGTI	Equipe da Oracle move as aplicações automaticamente para equipamentos sem problemas	Até 20 minutos
Falta de Energia no Datacenter (baixa)	PGTI	Equipe da Oracle move as aplicações automaticamente para equipamentos não afetados. O DC onde estão localizadas as aplicações atendem às melhores práticas de mercado para ambientes de Cloud Publica.	Até 20 minutos
Falta de Energia no Escritório (Média)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços e tomada de decisão se devem ou não ser liberados os usuários para home office. A estrutura de rede é toda protegida por Nobreaks e possui autonomia de 20	Até 2 horas

		minutos.	
Indisponibilidade da rede lógica (Baixa)	PGTI	Verificação dos equipamentos defeituosos e substituição dos mesmos. Os equipamentos são monitorados proativamente para diminuir ao máximo a indisponibilidade ao usuário.	Até 2 horas

15.3.2. Link de internet

O Grupo Fusão dispõe de 2 links de acesso a internet configurados em Failover. O principal é um link dedicado com SLA contratado, o secundário é um link banda larga de operadora local.

Risco e Probabilidade	Responsável da Fusão	Ação de Contingência	Tempo de Recuperação
Falha de Hardware (baixa)	PGTI	Abrir chamado com a operadora para a troca do mesmo. O link secundário é acionado automaticamente.	Até 1 minutos
Falta de Energia no Datacenter (baixa)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços e tomada de decisão se devem ou não ser liberados os usuários para home office. A estrutura de rede é toda protegida por Nobreaks e possui autonomia de 30 minutos.	Até 2 horas (deslocamento dos funcionários)

Falha de qualquer ponto na rede da Operadora (Equipamento, ruptura de fibra etc) (baixo)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços e tomada de decisão se devem ou não ser liberados os usuários para home office. O link secundário pode causar lentidão em alguns serviços.	Até 2 horas

15.3.3. Servidor de arquivos corporativo

Toda a estrutura de arquivos corporativa é baseada em Sharepoint Online.

Risco e Probabilidade	Responsável da Fusão	Ação de Contingência	Tempo de Recuperação
Falha de Hardware (baixa)	PGTI	Equipe da Microsoft move as aplicações automaticamente para equipamentos sem problemas	Até 20 minutos
Falta de Energia no Datacenter (baixa)	PGTI	Equipe da Microsoft move as aplicações automaticamente para equipamentos não afetados. O DC onde estão localizadas as aplicações atendem às melhores práticas de mercado para ambientes de Cloud Publica.	Até 20 minutos
Falta de Energia no Escritório (Média)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços e tomada de decisão	Até 2 horas

		se devem ou não ser liberados os usuários para home office. A estrutura de rede é toda protegida por Nobreaks e possui autonomia de 30 minutos.	
Indisponibilidade da rede lógica (Baixa)	PGTI	Verificação dos equipamentos defeituosos e substituição dos mesmos. Os equipamentos são monitorados proativamente para diminuir ao máximo a indisponibilidade ao usuário.	Até 2 horas

15.3.4. Sistema de E-mail

Toda a estrutura de e-mails corporativa é baseada em Exchange online atualmente na infraestrutura da MANDIC.

Risco e Probabilidade	Responsável da Fusão	Ação de Contingência	Tempo de Recuperação
Falha de Hardware (baixa)	PGTI	Equipe da Mandic move as aplicações automaticamente para equipamentos sem problemas	Até 20 minutos
Falta de Energia no Datacenter (baixa)	PGTI	Equipe da Mandic move as aplicações automaticamente para equipamentos não afetados. O DC onde estão localizadas as aplicações atendem às melhores práticas	Até 20 minutos

		de mercado para ambientes de Cloud Publica.	
Falta de Energia no Escritório (Média)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços e tomada de decisão se devem ou não ser liberados os usuários para home office. A estrutura de rede é toda protegida por Nobreaks e possui autonomia de 30 minutos.	Até 2 horas
Indisponibilidade da rede lógica (Baixa)	PGTI	Verificação dos equipamentos defeituosos e substituição dos mesmos. Os equipamentos são monitorados proativamente para diminuir ao máximo a indisponibilidade ao usuário.	Até 2 horas

15.3.5. Sistema de autenticação de usuários (AD)

O Grupo Fusão dispõe de Servidores Físicos para infraestrutura local. Estes servidores são hospedeiros das máquinas virtuais responsáveis pela autenticação de usuários.

Risco e Probabilidade	Responsável da Fusão	Ação de Contingência	Tempo de Recuperação
Falha de Hardware (baixa)	PGTI	Verificação da falha, análise de tempo de recuperação. Caso	Até 1 minuto

		seja necessária aquisição de equipamentos ou materiais a equipe da PGTI fará os orçamentos e enviará ao responsável. As aplicações funcionam em redundância nos dois servidores físicos, logo o usuário não percebe a falha.	
Falta de Energia no Datacenter (baixa)	PGTI e lideranças do Grupo Fusão	Verificação dos motivos e tempo de retorno estimado pela fornecedora de serviços. A estrutura de rede é toda protegida por Nobreaks e possui autonomia de 30 minutos. O serviço de autenticação funciona em cache na máquina do usuário, não causando problemas no trabalho.	Até 2 horas
Vírus ou ataque de hackers (médio)	PGTI	Todos os sistemas possuem soluções de antivírus de nível empresarial e são atualizados conforme análise da equipe responsável. Em caso de qualquer	Até 3 horas

		problema a máquina virtual é derrubada e é restaurada ao último checkpoint confiável.	

16. POLÍTICA DE PRIVACIDADE

Esta Política de Privacidade tem a finalidade de apontar, em um único local, todas as informações a respeito do uso das informações e dados pessoais, considerando os mais variados produtos e serviços disponibilizados. Em outras palavras, esta Política tem o intuito de explicar sobre como trataremos os dados pessoais em nossos sistemas.

E, se, após a leitura desta Política, ainda existirem dúvidas, entrar em contato conosco por meio do seguinte e-mail: **alessandro.rodrigues@fusao.com**. Não recomendamos o uso de nossas Plataformas, produtos e serviços caso você não concorde com os termos desta Política de Privacidade, uma vez que, em certos casos, o tratamento de dados pessoais é necessário para cumprir nossa parte e fornecer nossos produtos e serviços com a melhor qualidade possível.

16.1. Como coletamos os dados pessoais?

Podemos coletar os dados pessoais da seguinte forma:

16.1.1. Identificadores eletrônicos (cookies)

Cookies são basicamente arquivos de internet que podem ser temporariamente armazenados em seus dispositivos. Nós utilizamos cookies para facilitar sua navegação em nossas Plataformas, adequando-as a seus interesses e necessidades, por exemplo, por meio da personalização de conteúdo. Eles também são importantes para nos fornecer informações sobre como nossos websites e nossos serviços estão sendo utilizados.

Você pode configurar seu dispositivo para não aceitar ou recusar o uso de cookies. Nesse caso, você não conseguirá acessar todas as páginas de nossas Plataformas, já que alguns cookies são essenciais para o funcionamento adequado delas.

16.1.2. Mídias Sociais

Você pode, também, interagir conosco por meio de nossas páginas em mídias sociais de terceiros. Neste caso, poderemos armazenar informações como seu nome de usuário e o conteúdo da mensagem, para melhor atendê-lo.

16.1.3. Dados pessoais transferidos por nossos parceiros comerciais

Eventualmente, você pode contratar um de nossos produtos ou serviços por meio de nossos parceiros comerciais e, nesses casos, seus dados pessoais serão fornecidos por estes terceiros para que nós possamos oferecer de maneira especifica os nossos produtos e prestar nossos serviços a você.

16.1.4. Dados de cadastro ou de contato

Você pode fornecer para nós dados pessoais de maneira direta, ao nos contatar, ao se cadastrar em nossas Plataformas, ou contratar algum(ns) de nossos produtos e/ou serviços. Nesse caso, nós utilizaremos esses dados especificamente para a finalidade que eles foram coletados, ou seja:

- Se você nos contatou para solicitar informações ou esclarecimentos sobre nossos produtos e serviços, nós utilizaremos seus dados pessoais para respondê-lo de maneira apropriada;
- Se você se cadastrou para receber informações de novidades, atividades, eventos e cursos. que podem ser de seu interesse, então nós utilizaremos seus dados para fornecer essas informações;
- Se você forneceu seus dados ao receber nossa newsletter ou ao se inscrever em algum de nossos eventos, então utilizaremos seus dados pessoais para cumprir com nossas obrigações contratuais.

Sempre que possível, nós tentaremos fornecer a você opções razoáveis em relação à coleta e ao uso de suas informações. Por exemplo, você pode:

- Não fornecer dados pessoais que não sejam necessários para (i) a prestação de nossos serviços e (ii) o cumprimento de obrigações legais ou contratuais;
- Definir suas preferências de navegação e utilizar ferramentas disponíveis para bloquear os cookies enviados em conexão com seu uso de nossos websites e aplicativos;

- Optar pelo não recebimento de nossas comunicações de publicidade por meio de e-mail;
- Enviar uma solicitação relacionada ao exercício de seus direitos para o seguinte e-mail: **alessandro.rodrigues@fusao.com**.

16.2. Quais dados pessoais são coletados, e para qual finalidade?

O Grupo Fusão se preocupa em garantir que apenas as informações mínimas necessárias dentro do propósito de tratamento sejam coletadas e que seja claramente comunicado ao titular.

- Informações cadastrais como Nome, CPF, RG, Filiação, e-mail, data de nascimento, telefone, endereço e informações bancárias utilizadas para cadastro, e filiação ao sindicato.
- Nome, CPF e RG com solicitação do contratante para os materiais fornecidos pelo Grupo Fusão.
- Dados de identificação digital como Endereço de IP, Registros de interações com nossos websites, Sistema operacional utilizado e Geolocalização para cumprir obrigações legais e regulatórias, identificação do usuário e suas preferências de navegação, avaliação geral sobre como nossas Plataformas e Serviços são utilizados, e como podemos melhorá-los, para fins de análise estatística e de segurança e para publicidade digital personalizada.

16.3. Com quem compartilhamos seus dados pessoais?

Para que seja possível disponibilizar nossos produtos e serviços, precisaremos compartilhar dados pessoais com terceiros.

Podemos divulgar seus dados pessoais para:

- Nossas subsidiárias, coligadas e afiliadas;
- Contratados, prestadores de serviço e outros terceiros que contratamos para suportar nossos negócios, e que, portanto, estão contratualmente vinculados a nós;
- Pontualmente, com o seu consentimento, para qualquer outra finalidade divulgada por nós no momento de coleta dessas informações;

- Qualquer autoridade governamental competente, por exemplo, para o cumprimento de qualquer ordem judicial, lei, processo legal ou administrativo;
- Nossos parceiros comerciais, no cumprimento de nossos contratos e acordos;

16.4. Exercício de seus direitos

Você pode nos contatar diretamente para exercer quaisquer de seus direitos garantidos por lei, como o acesso aos dados pessoais que temos sobre você, a confirmação da existência de uma atividade de tratamento de dados pessoais, a revisão de decisões automatizadas, a correção de seus dados pessoais, a portabilidade, a anonimização, bloqueio ou eliminação de dados pessoais (nesses três últimos casos apenas se os dados pessoais forem excessivos ou tratados em desconformidade com a lei).

Podemos não aceitar um pedido de alteração de seus dados pessoais, se, por exemplo, acreditarmos que a alteração violaria uma lei ou tornaria alguma outra informação incorreta. O acesso e uso adequados das informações fornecidas em nossas Plataformas são regidos pelos nossos Termos de Uso e pela legislação em vigor.

Por favor, note que se você excluir seus dados pessoais, poderemos manter uma cópia armazenada em nossos arquivos, nos casos exigidos por lei, ou se tivermos uma base legal que autorize a conservação de tais dados pelo período garantido em lei.

A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I – em formato simplificado, **em até 48 horas**;

II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de **até 15 (quinze) dias**, contado da data do requerimento do titular.

16.5. Os seus direitos

A Fusão Soluções para Medicina Ltda permite, por parte do cliente e usuários, todos os direitos relativos ao tratamento de seus dados pessoais previstos na legislação, principalmente os seguintes:

- Solicitar a confirmação da existência de tratamento e o acesso aos dados que o Grupo Fusão possui sobre você;
- Solicitar a retificação ou atualização dos dados pessoais inexatos ou desatualizados;
- Solicitar a exclusão de suas informações pessoais existentes em nosso banco de dados e dos nossos parceiros, exceto nas hipóteses em que esse direito possa ser limitado conforme determina a lei;
- Solicitar a portabilidade de seus dados pessoais num formato estruturado, de uso corrente e de leitura automática, a outro fornecedor de serviço ou produto, mediante sua solicitação;
- Retirar, a qualquer momento, o seu consentimento, para os fins para os quais este foi obtido.
- Se você deseja exercer algum dos seus direitos em relação às suas informações pessoais ou se tiver alguma dúvida sobre como usamos suas informações pessoais, entre em contato conosco por meio da área de Contato de nosso website:
- DPO: Alessandro Rodrigues

16.6. Segurança dos Dados Armazenados

Nossa responsabilidade é cuidar dos dados pessoais, e utilizá-los somente para as finalidades descritas nessa Política. E para garantir a sua privacidade e a proteção dos seus dados pessoais, adotamos as práticas de segurança adequadas para nosso mercado.

O Grupo Fusão. se esforça para proteger a privacidade dos seus dados pessoais. Mantemos salvaguardas de caráter procedimental, técnico e físico que nos ajudam a evitar a perda, uso indevido ou acesso não autorizado, divulgação, alteração ou destruição dos dados pessoais fornecidos.

Todas as interações de nossos funcionários com informações sensíveis são mointoradas por sistemas de controle de acesso, modificação e proteção

contra perda de dados. No caso de informações físicas em nossa posse as interações são catalogadas.

17. OFICIAL DE PROTEÇÃO DE DADOS (DPO)

17.1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

17.1.1. Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados;

17.1.2. Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

17.1.3. Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos da LGPD;

17.1.4. Coopera com a autoridade de controle;

17.1.5. Ponto de contato para a autoridade de controle sobre questões relacionadas com o tratamento e consultadas informações.

17.2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

Em síntese, o DPO está incumbido de

i) treinar e orientar os funcionários da organização em sobre os requisitos de conformidade com LGPD;

ii) realizar avaliações e auditorias regulares para garantir a conformidade com o LGPD;

iii) servir como ponto de contato entre a empresa e a autoridade supervisora;

iv) manter registros das atividades de processamento de dados realizadas pela organização;

v) responder e informar os titulares de dados pessoais sobre como seus dados estão sendo usados e quais medidas de proteção implementadas pela organização e,

vi) assegurar que os pedidos de acesso ou apagamento de dados feitos por titulares de dados pessoais, sejam atendidos ou respondidos, conforme necessário.

18. DISPOSIÇÕES FINAIS

18.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma ao Gestor de Segurança da Informação – Arley Beu.

18.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Gestor de Segurança da Informação – Arley Beu deve ser imediatamente notificado a fim de adotar as providências necessárias.

18.3. Os incidentes de segurança, quebra de segurança e denúncias de descumprimento à Política de Segurança da Informação e suas normas podem ser encaminhadas através do e-mail gestordesegurança@fusao.com.

18.4. Os usuários que se depararem com incidentes que afetem a segurança de ativos ou descumprimento desta norma devem coletar as evidências através de print de tela, encaminhamento de e-mail, cópia de textos em casos de mensagem de erros ou quaisquer outros meios disponíveis de modo a garantir que a mesma não se perca e enviar ao Gestor de Segurança da Informação – Arley Beu.

18.5. Todas as informações coletadas pelo Gestor de Segurança da Informação – Arley Beu serão analisadas pela equipe de TI e o resultado desta análise será levado ao Comitê de Gestão de Segurança para análise das ações.

18.6. Esta política deve ser revisada anualmente ou quando existir a necessidade, pelo comitê de Segurança da Informação.

18.7. Qualquer modificação nas políticas deve ser oficialmente noticiada pelo setor de comunicação do Grupo Fusão.

18.8. Deverá ser realizado treinamento anual de atualização das políticas e conscientização dos funcionários do Grupo Fusão quanto à importância da segurança da informação e privacidade de informações. Neste treinamento devem ser abordados todos os aspectos desta política, além de fatores de comportamento para garantir a segurança e compliance do Grupo Fusão.