DIEFRA

DIEFRA ENGENHARIA E CONSULTORIA LTDA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BELO HORIZONTE

2023

DIEFRA

SUMÁRIO

1. APRESENTAÇÃO

As informações da Diefra, colaboradores e parceiros são bens que requerem proteção e tratamento de forma ética e sigilosa, de acordo com a legislação vigente e as normas internas da empresa, evitando-se o mau uso, a perda e a exposição indevida.

Entende-se por informação, não apenas o que está armazenado nos computadores, redes ou sistemas utilizados pela empresa, mas, também, o que foi impresso ou salvo em mídias digitais e, ainda, o que foi transmitido através de meios eletrônicos ou de conversas em ambientes internos e externos à empresa. O efetivo cumprimento da Política de Segurança da Informação - PSI é uma importante ferramenta para combater ameaças a estes ativos da empresa.

2. OBJETIVO

Esta PSI é um conjunto de diretrizes que visa conscientizar e orientar os colaboradores, parceiros e clientes da Diefra para o uso seguro da informação, garantindo a observância aos princípios inerentes à segurança da informação, quais sejam:

a) **Integridade:** salvaguarda da exatidão e correção da informação, bem como dos métodos de processamento;

b) **Confidencialidade:** propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

c) **Disponibilidade:** propriedade da informação estar acessível e utilizável sempre que necessário;

d) **Autenticidade:** garantia de que seja identificado e registrado o usuário que está enviando ou modificando a informação.

As orientações aqui apresentadas são os princípios fundamentais e representam como a Diefra exige que a informação seja utilizada.

3. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da organização cientificando-os de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados, em qualquer tempo e circunstância.

É obrigação de cada colaborador manter-se atualizado em relação a esta política e aos procedimentos e normas a ela relacionadas, buscando orientação do seu gestor, do comitê de proteção de dados, da área de compliance ou da área de TI sempre que não estiver seguro quanto às diretrizes aqui apresentadas.

Deverá constar em todos os contratos com parceiros da Diefra, cláusula de confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela organização.

O cumprimento da política de segurança pelos colaboradores, clientes e parceiros poderá ser auditado pela Diefra.

4. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

Esta política define as diretrizes para a segurança da informação, visando preservar a integridade, confidencialidade, autenticidade e disponibilidade das informações sob gestão da Diefra. Descreve a conduta

considerada adequada para o manuseio, controle e proteção das informações, contra acessos não autorizados, destruição, modificação e divulgação indevida, seja acidental ou intencionalmente. As condutas aqui estabelecidas estão em total consonância com o código de ética da empresa.

4.1. PROPRIEDADE DA INFORMAÇÃO

Toda informação produzida, acessada, recebida, manuseada ou armazenada pelos colaboradores, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e de direito de uso exclusivos Diefra, sendo, portanto, proibidas as cópias, reproduções ou distribuições sem a devida autorização. As exceções devem ser explícitas e formalizadas por meio de email pelo gestor responsável da área ou unidade.

A utilização da marca, identidade visual e demais sinais distintivos da Diefra, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só poderá ser feita para atender às atividades profissionais da organização.

4.2 CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade de cada gestor estabelecer critérios relativos ao nível de confidencialidade da informação gerada ou recebido por sua área, de acordo com os critérios a seguir:

a) **Pública:** Informações da empresa com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo,

comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação;

b) **Corporativa:** Informações cujo conhecimento é de interesse de toda a empresa, podendo ser divulgada para beneficiários, participantes e parceiros;

c) **Uso Interno:** Informações de conhecimento exclusivo dos colaboradores da organização e deve ser divulgada apenas para o público interno;

d) **Restrita:** É toda informação que pode ser acessada somente por colaboradores de áreas previamente definidas.

e) **Confidencial:** É uma informação crítica para os negócios da organização ou de parceiros, devendo haver indicação do nome ou cargo do colaborador responsável. A divulgação não autorizada desta informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e/ou criminais.

4.3. UTILIZAÇÃO, GUARDA E DESCARTE DE DOCUMENTOS

Documentos que contenham informações classificadas como uso interno, restrita ou confidencial não podem ficar expostos na estação de trabalho, em impressoras, fax, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião.

Documentos que contenham informações classificadas como restrita ou confidencial devem ser acondicionados em armários de acesso controlado, sua destruição, quando for o caso, deverá ser feita por meio de triturador de papel.

Nenhuma das informações restritas ou confidenciais podem ser repassadas para terceiros sem consentimento formalizado pela gerência, superintendência ou diretoria da Diefra.

É expressamente proibida a divulgação de informações dos participantes e beneficiários.

As áreas devem observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia da gerência, superintendência ou diretoria responsável.

A empresa de guarda externa deverá emitir certificado ou declaração de destruição segura dos documentos indicados pela organização.

4.4. BACKUP (CÓPIAS DE SEGURANÇA)

Os backups devem ser realizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial, período em que não há nenhum ou pouco acesso de usuários ou processos automatizados dos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.

Além dos backups normalmente realizados no servidor, quando localizado em um datacenter on-premise, deverá ser feito backup adicional mantido em dispositivo externo com as informações codificadas (encriptografadas) em ambiente seguro para armazenagem fora da Diefra. Quando em cloud, o acompanhamento deverá ser realizado através da ferramenta de gestão do ambiente do fornecedor. O fornecedor deverá fornecer

cópia do certificado de segurança do ambiente, garantindo assim a eficiência e segurança da solução entregue ao cliente.

4.5. CONTROLES DE ACESSO/LOGINS

Para cada colaborador da Diefra deverá ser fornecido logins de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa. O colaborador é responsável por todas as atividades desenvolvidas por meio de seus logins de acesso pessoal. É vedada, a qualquer colaborador, a utilização de login de acesso pessoal de outro colaborador mesmo quando cedida por este.

É de responsabilidade de cada colaborador da organização a guarda dos logins de acessos que lhe forem designados, bem como, a memorização de sua própria senha. As senhas não devem ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da organização, nome do departamento e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. As senhas de acesso deverão ser trocadas ao menos semestralmente.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a organização e a legislação (cível e criminal) será dos colaboradores que dele se utilizarem.

A concessão de acessos deverá seguir o critério de menor privilégio, no qual os colaboradores tenham acesso apenas às informações imprescindíveis para o pleno desempenho de suas atividades.

Cada gerente de área deverá, através do helpdesk, solicitar à equipe de TI inclusões, alterações ou exclusões de acesso a usuários, definindo os

serviços que deverão ser incluídos, alterados ou excluídos e justificando quanto à necessidade da solicitação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, a Equipe de TI deverá ser comunicada via helpdesk para providenciar o imediato cancelamento de todas as suas senhas de acesso a equipamentos e sistemas corporativos, bem como de seu e-mail, sendo esse comunicado previamente pela gerência responsável pelo colaborador desligado ou transferido de área.

4.6. SEGURANÇA DO AMBIENTE FÍSICO

É vedado o acesso de pessoas não autorizadas ao Data Center, ou equivalente, da Diefra.

O acesso de visitantes às áreas internas da Diefra deverá ser supervisionado pelo gestor da área responsável.

As áreas de acesso restrito, somente podem ser acessadas por colaboradores devidamente autorizados.

O acesso às dependências da organização com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho, somente poderá ser realizado a partir de autorização da gerência, superintendência ou diretoria e mediante supervisão.

Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar e / ou compartilhar imagens dos ambientes internos da Diefra que possam:

a) Comprometer a segurança dos demais colaboradores;

b) Comprometer o sigilo das informações;

c) Impactar negativamente a imagem da Diefra, outros colaboradores, clientes, parceiros e/ou visitantes.

4.7. MESA LIMPA / TELA LIMPA

Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27.001 da Mesa limpa / Tela limpa. Este princípio tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. A adoção de uma política de “mesas limpas” para os papéis e mídias de armazenamento removível e, igualmente, uma política de “telas limpas”, contra, por exemplo, o perigo de ter um usuário já autenticado / registrado, porém ausente e com sua sessão de trabalho aberta. A política de Mesa Limpa / Tela Limpa busca resguardar a Diefra bem como o próprio usuário contra o acesso não autorizado a informações como, por exemplo, terceiros observando dados expostos em mesas ou telas. Assim, sinteticamente, entre outros:

a) Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);

b) Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente ficar vazio;

c) Computadores e notebooks não devem ser deixados autenticados / registrados quando não houver um colaborador (operador) junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso (tela limpa);

d) Informações restritas ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;

e) Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;

f) Papéis, livros ou qualquer informação restrita ou confidencial não devem ser deixados na mesa;

g) Informações restritas ou confidenciais devem ser mantidas em local apropriado (longe dos olhos de curiosos);

h) Bloqueio de tela que solicite uma senha para acesso deve ser usado;

i) Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados / organizados, com proteção adequada;

j) Documentos contendo informações pessoais devem ser mantidos trancados.

4.8. SEGURANÇA DOS EQUIPAMENTOS

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI ou de quem esta determinar.

Os sistemas e computadores devem ter versões de software antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de hardware ou software, o colaborador deverá acionar a área de TI da Diefra via helpdesk.

Os colaboradores deverão proteger o acesso a seus computadores por meio de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso. Ao final do expediente de trabalho diário, o computador deverá ser desligado.

4.9. UTILIZAÇÃO DA REDE E GOOGLE DRIVE

A Diefra possui uma rede integrada de computadores com servidores de autenticação de usuários e impressão, e um microcomputador/notebook para cada colaborador alocado na matriz, além de acesso ao drive compartilhado do Google para atender colaboradores da matriz e obras.

O acesso à rede da Diefra só poderá ser efetivado após o registro obrigatório de computadores e usuários, de acordo com os sistemas de registro implementados e para acesso ao drive compartilhado do Google através de autenticação via conta de e-mail corporativo de cada colaborador.

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso.

Os colaboradores da Diefra não deverão obter ou disponibilizar material sem a licença adequada através da rede.

O usuário é responsável pela própria e devida autenticação nos sistemas de redes e acesso ao drive compartilhado do Google disponibilizados pela Diefra, não podendo fornecer e / ou compartilhar seu usuário, senha e / ou acessar com outros usuários.

O usuário está comprometido a utilizar a rede interna da Diefra e drive compartilhado do Google para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence.

É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas.

Os usuários devem administrar suas pastas, excluindo arquivos desnecessários.

Material sexualmente explícito ou contrário à legislação brasileira não podem ser expostos, armazenados, distribuídos, editados ou gravados, através do uso dos recursos computacionais da rede corporativa da empresa.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc..) nos drivers de rede e drive do Google. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação.

4.10. UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS

Os sistemas corporativos são os sistemas utilizados na gestão Diefra, os quais buscam trazer maior transparência, tempestividade e confiabilidade para as informações, abrangendo todos os segmentos da administração da organização e permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados por meio de uma rede interna ou externa.

É expressamente proibida a divulgação e / ou o compartilhamento indevido das informações contidas nos sistemas corporativos da Diefra.

Todos os usuários dos ativos de informação de propriedade da Diefra, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do mesmo, mantendo conduta profissional.

O acesso às informações contidas nos sistemas corporativos deve ser efetuado sempre através de identificação segura (login e senha).

Para cada usuário devem ser atribuídas permissões específicas, por módulo e/ou operação.

A concessão de acesso às bases de dados para prestadores de serviço e colaboradores deverá sempre seguir o critério do menor privilégio possível.

4.11. UTILIZAÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA E COMUNICAÇÃO

Os equipamentos de informática e de comunicação são utilizados pelos colaboradores da empresa para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Diefra, por meio de sua área de TI, poderá registrar todo e qualquer uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores, os quais deverão assinar um termo de responsabilidade dos equipamentos e confidencialidade das informações.

Os acessos ao drive compartilhado do Google possuem rastreabilidade de todas as atividades executadas por cada colaborador, sendo assim é de responsabilidade de cada colaborador zelar pelos seus respectivos acessos.

4.12. UTILIZAÇÃO DA INTERNET

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

A internet, via cabo ou Wi-Fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da Diefra.

O colaborador é responsável pelas atividades realizadas por intermédio de seu login e senha de acesso. Em particular, o usuário deverá observar os termos de licença de uso do material obtido através da internet.

Os colaboradores da Diefra não deverão:

a) Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente política, lesivos aos direitos e interesses da organização ou de terceiros;

b) Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os recursos de tecnologia da informação e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros;

c) Acessar a sites de proxy com o objetivo de burlar os mecanismos de segurança existentes;

d) Acessar sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, ainda que os mesmos não estejam bloqueados no sistema de segurança da organização.

Os equipamentos fornecidos para o acesso à internet são de propriedade da Diefra ou de responsabilidade da mesma através de um contrato de locação de terceiros. Assim, a organização poderá analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados em disco local, na rede ou internet.

Assim, a organização, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

4.13. UTILIZAÇÃO DE E-MAIL (CORREIO ELETRÔNICO)

Os serviços de correio eletrônico são oferecidos como um recurso profissional pela Diefra para seus colaboradores no cumprimento de seus objetivos nas áreas de atuação.

O uso pessoal poderá ser permitido, mas não priorizado, desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades, não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da Diefra, não incorra em gastos adicionais para a organização, ou viole qualquer outra lei ou norma vigente.

Portanto, cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal.

O acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros.

Os colaboradores e parceiros com acesso, aos serviços de mensagem eletrônica disponibilizados pela Diefra devem observar o seguinte:

a) Todos os usuários dos ativos de informação de propriedade da Diefra, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da organização, mantendo uma conduta ética e profissional;

b) Todas as contas de e-mail terão uma titularidade, sendo o usuário titular o responsável direto pelas mensagens enviadas por intermédio do seu endereço de e-mail;

c) O usuário deve utilizar o e-mail de forma adequada e diligente;

d) É vedado o envio, armazenamento ou manuseio de material que caracterize a divulgação, incentivo ou prática de atos que:

- Contrariem o disposto na legislação vigente, ética, moral e de ordem pública;

- Sejam proibidos pela presente Política, lesivos aos direitos e interesses da Diefra ou de terceiros;
- De qualquer forma, possam danificar, inutilizar, invadir, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
- Promovam ameaças, difamação ou assédio a outras pessoas;
- Cotenham conteúdo considerado impróprio, obsceno ou ilegal;
- Sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenham a prática de qualquer tipo de discriminação relativa a raça, sexo, credo religioso, incapacidade física ou mental ou outras situações protegidas;
- Caracterize violação de direito autoral garantido por lei.

e) É vedada ainda a utilização do e-mail, nas situações abaixo:

- Acesso não autorizado à caixa postal de outro usuário;
- Uso para atividades com fins comerciais ou políticos e o uso extensivo para assuntos pessoais ou privados;
- Envio de mensagens do tipo “corrente” e “spam”;
- Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
- Utilização de grupos de endereços da Diefra para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão da área de TI pelos grupos de endereços em questão;

- Divulgação de informações em não conformidade com a diretriz de classificação de informações prevista nesta política;
- Envio de qualquer mensagem que torne a organização vulnerável a ações civis ou criminais;
- Exclusão de mensagens relacionadas às atividades profissionais, quando a organização ou pessoas a ele relacionadas estiverem sujeitos a algum tipo de investigação.

A Diefra possui instrumentos para o bloqueio ou cópia de mensagens de maneira a subsidiar processos internos de sindicância ou para atendimento de ordem judicial.

O bloqueio poderá ser aplicado a recepção de mensagens provenientes de alguns locais, comerciais ou não, em caso de inconveniência e/ou possível ameaça contida em mensagens indesejáveis.

Os usuários devem utilizar em sua assinatura padrão texto que identifica os requisitos de segurança da informação relacionados à confidencialidade da troca de informações, servindo como instrução a terceiros que recebam mensagens provenientes da Diefra.

“AVISO: A informação contida neste e-mail, bem como em qualquer de seus anexos, é CONFIDENCIAL e destinada ao uso exclusivo do (s) destinatário (s) acima referido (s), podendo conter informações sigilosas e/ou legalmente protegidas. Caso você não seja o destinatário desta mensagem, informamos que qualquer divulgação, distribuição ou cópia deste e-mail e/ou de qualquer de seus anexos é absolutamente proibida. Solicitamos que o remetente seja comunicado imediatamente, respondendo esta mensagem, e que o original desta mensagem e de seus anexos, bem como toda e qualquer cópia e/ou impressão realizada a partir destes, sejam permanentemente apagados e/ou destruídos. Informações adicionais sobre nossa empresa podem ser obtidas no site http://www.diefra.com.br/.

NOTICE: The information contained in this e-mail and any attachments thereto is CONFIDENTIAL and is intended only for use by the recipient named herein and may contain legally privileged and/or secret information. If you are not the e- mail´s intended recipient, you are hereby notified that any dissemination, distribution or copy of this e-mail, and/or any attachments thereto, is strictly prohibited. Please immediately notify the sender replying to the above mentioned e-mail address, and permanently delete and/or destroy the original and any copy of this e-mail and/or its attachments, as well as any printout thereof. Additional information about our company may be obtained through the site http://www.diefra.com.br/."

4.14. UTILIZAÇÃO DE SOFTWARE DE MENSAGENS INSTANTÂNEAS/REDES SOCIAIS

Os serviços de comunicação instantânea instalados nos equipamentos serão inicialmente disponibilizados aos colaboradores que necessitem dessa ferramenta e poderão ser bloqueados, caso o gestor requisite formalmente à área de TI da organização.

O uso de aplicativos de comunicação pelos colaboradores, a partir de recursos da Diefra, para compartilhar informações profissionais, deverá ser feito de forma responsável para evitar riscos desnecessários, que possam comprometer as atividades, os projetos ou a própria organização.

O colaborador deve, ainda, sempre que possível, preservar o sigilo e a confidencialidade das informações, atender aos requisitos de segurança previstos nesta política e respeitar a legislação vigente.

4.15. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS

Dispositivos móveis corporativos são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória.

É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos.

O usuário deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativos, tanto por sua guarda, quanto pelos conteúdos neles instalados.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo. Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um colaborador da área de TI.

O colaborador deverá responsabilizar-se por não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados por um colaborador da área de TI.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Diefra, notificar imediatamente seu gestor e a

área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na Delegacia de Furtos de Roubos (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a organização e/ou a terceiros.

Em caso de desligamento, o colaborador deve realizar imediata devolução de seus dispositivos móveis à área de TI e assinar o termo de devolução do equipamento.

4.16. UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS

O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que tais dispositivos possam vir a causar, uma vez que esse tipo de mídia pode conter vírus e softwares maliciosos, capazes de danificar e corromper dados.

4.17 ACESSO REMOTO AO HOSTING

O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da Diefra e/ou terceiros que utilizam serviços de acesso

remoto. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da organização. O usuário somente poderá realizar as atividades em período estipulado pela Diefra e devidamente autorizado por seu gestor.

4.18. ACESSO REMOTO À REDE DA DIEFRA

A interconexão entre redes privadas a distância permite ao usuário utilizar-se de redes e serviços de redes disponibilizados por terceiros. O acesso a redes remotas disponibilizadas por redes privadas externas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da Diefra e/ou terceiros que utilizam serviços de acesso remoto. Cabe enfatizar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da Diefra.

a) O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida;

b) O usuário deve utilizar somente o local e o ambiente físico aprovado pela Diefra;

c) O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede da Diefra;

d) O usuário somente poderá realizar as atividades em período estipulado pela Diefra e devidamente autorizado por seu gestor.

4.19. INSTALAÇÕES DE SOFTWARE

O colaborador da Diefra é proibido de instalar todo e qualquer programa não autorizado em seu computador e em qualquer outro dispositivo computacional pertencente à organização, salvo as instalações de programas que contenham prévia autorização da área de TI. Este comando também é aplicado a programas com conteúdo de atualização conhecidos como patches.

O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos onde exista uma versão atualizada da aplicação utilizada.

Caso o usuário necessite instalar ou remover qualquer software, deverá solicitar a área de TI via helpdesk.

Não é permitida a instalação / uso de softwares ilegais (sem licenciamento), sendo que a área de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da organização.

4.20. COMUNICAÇÃO VERBAL DENTRO E FORA DA ORGANIZAÇÃO

Somente os colaboradores que estão devidamente autorizados a falar em nome Diefra, para os meios de comunicação, podem fazê-lo em nome da organização.

A fim de evitar exposição desnecessária da Diefra, os colaboradores não devem tratar de assuntos internos em locais públicos ou dentro das instalações físicas da organização, quando próximos a visitantes ou terceiros.

4.21 ENGENHARIA SOCIAL

É um termo utilizado coloquialmente que representa a habilidade de enganar pessoas com o objetivo de obter informações sigilosas. Essa ação pode ocorrer de diversas formas, mas o comum é os engenheiros utilizarem a falta de conscientização dos colaboradores em relação à segurança da informação da organização. O ataque pode ser feito (i) de forma direta, quando há um contato entre o engenheiro social e a vítima, por meio de telefonemas ou pessoalmente, ou (ii) de forma indireta, quando há a utilização de softwares ou outras ferramentas, a fim de captar dados que facilitem o acesso às informações desejadas. Podem ser, por exemplo, mensagens que contenham avisos de premiações, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc.

Assim, se o colaborador suspeitar de um possível ataque, através dos meios tecnológicos, deverá comunicar imediatamente à área de TI. Caso a tentativa de ataque tenha ocorrido por outros meios (não tecnológicos), deverá ser comunicada ao comitê de proteção de dados.

5. RESPONSABILIDADES

A correta utilização dos recursos disponibilizados é dever de todos os colaboradores da organização, sendo que o uso indevido, negligente ou imprudente será responsabilizado, conforme normativos internos e legais. A Diefra reserva-se o direito de analisar dados e evidências, a fim de obter

provas, que possam ser utilizadas nos processos investigatórios, bem como, adotar as medidas legais cabíveis.

Quanto à presente política de segurança da informação da Diefra, as responsabilidades ficam assim distribuídas:

5.1. COMITÊ DE PROTEÇÃO DE DADOS

a) Determinar a adoção de medidas necessárias para o cumprimento da política;

b) Implantar e implementar a presente política;

c) Orientar e informar aos colaboradores as práticas necessárias à segurança da informação;

d) Receber o report de todo e qualquer usuário e/ou área para tratar de assuntos pertinentes à segurança da informação de que trata este instrumento;

e) Promover juntamente com a área de TI e os gestores dos processos a segregação de acessos necessários aos sistemas da Diefra, evitando conflitos de interesse e adotando perfis de acesso;

f) Receber e tratar as notificações dos casos de violação das diretrizes de segurança expostas neste instrumento;

g) Realizar testes e atualizações nos diversos acessos aos recursos de TI.

5.2. DIRETORIA EXECUTIVA

a) Promover a política de segurança e o cumprimento das normas aqui presentes.

5.3. SUPERINTENDÊNCIAS E GESTORES

a) Fazer cumprir as normas aqui presentes;

b) Assegurar que as equipes possuam acesso e conhecimento desta política;

c) Promover juntamente com a área de TI e o comitê de proteção de dados a segregação de acessos necessários aos sistemas da Diefra, evitando conflitos de interesse e adotando perfis de acesso.

5.4. ÁREA DE TI

a) Monitorar o ambiente de TI e a atividade de todos os usuários durante os acessos às redes internas e externas (internet), por exemplo: sites, e-mails, sistemas e outros;

b) Executar as ações necessárias para tratar violações de segurança no âmbito tecnológico;

c) Configurar os equipamentos, instalar softwares e implementar os controles necessários, bem como, definir regras para a instalação de software e hardware nos equipamentos da organização;

d) Coordenar as atividades de tratamento e resposta a incidentes de TI;

e) Promover a recuperação de sistemas, se necessário;

f) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos operacionais considerados críticos;

g) Planejar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida e a disponibilidade da rede interna;

h) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades na rede e nos equipamentos;

i) Promover juntamente com os gestores dos processos e a equipe de segurança da informação a segregação de acessos necessários aos sistemas da Diefra, evitando conflitos de interesse e adotando perfis de acesso;

j) Promover guarda de logs de auditoria dos sistemas da Diefra sempre que os mesmos fornecerem a referida possibilidade.

5.5. ÁREA DE CONTROLES INTERNOS

a) Avaliar os riscos do processo juntamente com os responsáveis;

b) Elaborar e executar planos de testes e realizar auditoria nos controles relacionados à segurança da informação;

c) Monitorar o resultado e sugerir novos controles no ambiente de segurança da informação, quando aplicável.

5.6. TODOS OS COLABORADORES DA ORGANIZAÇÃO

a) Conhecer e cumprir a presente política;

b) Assinar termo de ciência e responsabilidade sobre a política declarando ter conhecimento de suas responsabilidades;

c) Buscar orientação em caso de dúvidas relacionadas à segurança da informação;

d) Fiscalizar e orientar os parceiros e clientes da organização quanto às diretrizes desta política;

e) Observar os princípios constantes no Código de Ética;

f) Comunicar imediatamente quando do descumprimento ou violação desta política, conforme diretrizes do Item 7. Tratamento de Violações.

6. DIVULGAÇÃO E TREINAMENTO

O comitê de proteção de dados deverá definir um plano de divulgação e treinamento a fim de que todos os colaboradores estejam cientes das normas constantes na presente política.

Os colaboradores atuais e aqueles futuramente contratados deverão assinar termo de responsabilidade e confidencialidade, comprometendo-se a agir conforme as diretrizes aqui estipuladas.

7. TRATAMENTO DE VIOLAÇÕES

Os casos de violação das diretrizes de segurança expostas neste instrumento poderão ser notificados, conforme disposto abaixo:

1. Por meio do Fale Conosco – Ouvidoria, disponível no site da Diefra, quando ocorrência externa. Quando for uma ocorrência

interna, utilizar a ferramenta Helpdesk para registro de incidência de segurança.

2. Ao gestor de cada área;
3. O usuário infrator estará passível das seguintes penalidades imediatas, sem prévio aviso;
4. Descredenciamento da senha de acesso à Internet;
5. Cancelamento da conta de e-mail;
6. Cancelamento do acesso aos sistemas corporativos;
7. Desativação do ponto de rede do usuário.

O responsável por receber a notificação da transgressão deverá acionar imediatamente o comitê de proteção de dados, o qual fará a comunicação ao usuário infrator e à gerência, superintendência ou diretoria correspondente, para aplicação das penalidades previstas no código de ética da Diefra e na legislação vigente no Brasil.

8. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A gestão de continuidade de negócios define os procedimentos para prevenção de interrupções de atividades críticas ao negócio, viabilizando a ativação de processos alternativos na ocorrência de indisponibilidade dos serviços. Também visa orientar os colaboradores em relação aos procedimentos a serem realizados quando da ocorrência de algum incidente, informando as partes interessadas.

9. VIGÊNCIA, VALIDADE E ATUALIZAÇÕES

A presente política passa a vigorar a partir da data de sua aprovação pelo departamento de TI e Jurídico, sendo válida por tempo indeterminado.

Após a implantação desta política, com o objetivo de mantê-la atualizada e condizente com as necessidades da organização, deverão ser realizadas, anualmente, ou sempre que houver incidentes, revisões com a implantação de novas ações e controles para sua melhoria contínua.

10. TABELA DE CONTROLE DE REVISÕES

REVISÃO	DATA	MOTIVO	RESPONSÁVEL
1	28/04/2023	Atualização responsável	Edilson Araújo Leonardo Henrique Quites Teixeira

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação — Requisitos;

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

Manual de Governança em Segurança da Informação ABRAPP;

Plano Diretor de Tecnologia da Informação e Comunicação – SEBRAE PREVIDÊNCIA

Lei 9.609/98 - Lei do Software;

Lei 12.527/11 - Lei de Acesso à Informação;

Lei 12.737/12 - Lei Carolina Dieckmann;

Lei 12.965/14 - Marco Civil da Internet;

Lei 13.709/18 - Lei Geral de Proteção de Dados.

GLOSSÁRIO

1. **Ambiente Tecnológico:** Compreende todos os sistemas, computadores e redes do Instituto.
2. **Antivírus:** Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.
3. **Aplicativos de comunicação:** Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de Whatsapp, Telegram, Skype etc.
4. **Ativo:** Qualquer coisa que tenha valor para a organização e precisa ser adequadamente protegida.
5. **Backup:** É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
6. **Clientes:** Patrocinadores, instituidores, participantes e seus beneficiários.
7. **Data Center:** Rede de computadores utilizados para armazenamento, processamento ou distribuição remota de grandes quantidades de dados.
8. **Dispositivos móveis:** Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes. Exemplos: smartphone, notebook, tablet, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.
9. **Firewall:** Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

10. **Hardware:** conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador.
11. **Informação:** Conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno.
12. **Log:** Registro de eventos em um sistema de computadores.
13. **Mídias Removíveis:** Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
14. **Patches:** Programas criados para atualizar ou corrigir um software.
15. **Parceiros:** Pessoas Físicas ou Jurídicas que possuem relação de negócios com a organização.
16. **Peer-To-Peer (P2P):** Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.
17. **Perfil de Acesso:** Grupo de acessos a um recurso tecnológico estratificado por função dentro da organização.
18. **Colaboradores:** Corpo Diretivo, conselheiros, membros de comitê, empregados, estagiários e empregados terceirizados.
19. **Proxy:** Em redes de computadores, um proxy é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.
20. **RH:** Recursos Humanos.
21. **Sites de proxy:** Sites utilizados para acessar outros sites da web. Em redes corporativas que têm monitoramento ou bloqueio de sites, sites de proxy permitem a navegação anônima a sites proibidos.
22. **Servidor:** é um software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.

23. **Software:** É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores.
24. **SPAM:** Mensagem de e-mail publicada em massa com fins publicitários.
25. **TI:** Tecnologia da Informação.
26. **USB:** É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
27. **VDI (Virtual Desktop Infrastructure):** É um tipo de virtualização de desktops, utilizado para possibilitar o acesso a uma máquina virtual, onde o colaborador terá pleno acesso a todos os aplicativos disponibilizados pelo Instituto.
28. **VPN (Virtual Private Network):** Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por colaboradores autorizados em trânsito.
29. **Wi-Fi:** Abreviação de Wireless Fidelity - é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.