POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

VERSÃO 1.3

Antônio Barros Sobrinho
GERENCIA SOC

1.Objetivo

Assegurar a Nova a conformidade da Política de Segurança da informação esteja aderente a normas ISO 27001 e as leis pertinentes em vigor;

Proteger dados e informações como parte do patrimônio da empresa bem como aquelas sob a guarda, e todos os sistemas, aplicações e ferramentas que as modifiquem, armazene e processem as mesmas.

Atender em sua plenitude os fundamentos da ISO 27001 os quais são: Integridade, Disponibilidade e Confidencialidade das informações sob a guarda do grupo inclusive em meios não digitais;

Criar a cultura da Segurança da Informação a ser disseminada pelos Diretores, Gestores e demais colaboradores e terceiros.

Criar campanhas de divulgação da Política de Segurança da Informação com o objetivo de mantê-la perene na cultura da Nova.

2. Aplicação

Diretores, Gestores, funcionários, terceiros e clientes da Nova.

3. Definições

Segurança da Informação – É o conjunto de medidas, procedimentos, politicas, diretrizes e ferramentas destinadas a tornar a informação que uma vez entendida como um ativo da companhia tenha um elevado nível que atenda aos requisitos de confidencialidade, disponibilidade e integridade da mesma.

Confidencialidade - A informação deve ser acessada somente por pessoas autorizadas.

Integridade – A Informação deve manter seu conteúdo conforme a intenção de sua produção original.

Disponibilidade – A Informação deve estar disponível sempre que requerida por pessoas ou agentes que tenham permissão para utiliza-la

Autenticidade – A Informação deve ser autentica em sua forma.

Legalidade – A Informação de estar em conformidade com as regras, normas e leis vigentes.

Gestão da Segurança da Informação – Conjunto de pessoas e dispositivos responsáveis pela Informação.

4. Responsabilidades

Da Diretoria

Avaliar, aprovar e certificar-se que a Política de Segurança da Informação esteja alinhada com o Planejamento Estratégico da Empresa sendo o principal patrocinador desta;

Assegurar os recursos básicos para a Gestão da Segurança a Informação e do SOC estejam disponíveis, como sistemas de proteção e recursos humanos;

Da Gerencia de Segurança da Informação/SOC

Assegurar que o sistema e a forma de Gestão da Segurança da Informação e do SOC atinjam os resultados pretendidos;

Controlar o acesso, o bom uso e correto manuseio das informações e recursos digitais ou não da empresa criando mecanismos que possam servir de indicadores destes e consequentemente da eficiência da Política de Segurança da Informação.;

Comunicar os Gerentes de área e outros responsáveis sobre qualquer irregularidade ou incidente de Segurança relativo as mesmas;

Criar e manter equipe e comitê de “Resposta a Incidentes de Segurança”;

Manter os dados da empresa e dos clientes guardados em segurança seja em meio eletrônico ou não mantendo a conformidade com a **Lei Geral de Proteção de Dados;**

Garantir e controlar os recursos computacionais disponibilizados pela empresa;

Planejar campanhas de conscientização sobre a importância da Política de Segurança da Informação para funcionários, terceiros e gerentes;

Do RH

Comunicar contratações, movimentações e desligamentos de funcionários de forma que acessos aos recursos computacionais sejam criados, alterados ou revogados conforme o caso;

Dos Colaboradores e terceiros

Cumprir a Política de Segurança da Informação, zelando pelo uso correto não só dos equipamentos de tecnologia da informação, bem como o trato das informações, entendendo que estas também fazem parte do ativo da empresa

A Politica

Este documento estabelece a " Política de Segurança da Informação" da **Nova,** que é um conjunto das diretrizes, normas e procedimentos necessários à preservação e segurança das informações.

A Informação é um ativo, como qualquer outro ativo importante do negócio, que tem um valor para a companhia e consequentemente necessita ser protegida. A Segurança da Informação visa protegê-la de ameaças, de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e oportunidades.

A Informação pode existir em muitas formas: pode ser impressa ou escrita em papel; guardada eletronicamente; transmitida pelo correio ou usando meios eletrônicos; mostrada em filmes, ou falada em conversação. Seja qual for a forma tomada pela Informação, ou meio através do qual ela é compartilhada ou armazenada, ela deve ser protegida.

A Segurança da Informação é caracterizada pela **Confidencialidade, Integridade, Disponibilidade das Informações.**

A Segurança da Informação é alcançada a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais, instalações, softwares e ferramentas de controle automatizadas. Estes controles devem ser estabelecidos para garantir que os objetivos de segurança da organização sejam alcançados.

Abaixo alguns riscos típicos que a Política de Segurança da Informação pretende eliminar ou mitigar:

- **Revelação de Informações sensíveis;**
- **Modificações indevidas de dados e programas;**
- **Perda de dados e programas;**
- **Destruição ou perda de recursos computacionais e instalações;**
- **Interdições ou interrupções de serviços essenciais;**
- **Roubo de propriedades, seja qual for.**

As ameaças a serem tratadas são com relação a:

- **Integridade**: Prever ameaças de ambiente, externas ou internas, oriundas de catástrofes, fenômenos da natureza e qualquer evento provocado intencionalmente ou não. Cita-se aqui, como exemplo, fogo, enchentes, tempestades, inundações entre outros definidos em documento complementar de "Plano de Continuidade de Negócios" e "Plano de Recuperação de Desastres".

- **Indisponibilidade**: Prever falhas em sistemas e /ou diversos ambientes computacionais da organização.

- **Divulgação da Informação**: Prever a divulgação de Informações sensíveis aos Processos de Negócio da organização, premeditada e/ou acidental.

• **Alterações não autorizadas**: Prever alterações não autorizadas, premeditadas elou acidentais em Sistemas elou equipamentos de Tecnologia da Informação ou que suportem os Processos de Negócio.

Declaração de comprometimento da Direção, colaboradores e terceiros

As Direções da Nova, bem como seus Gestores, colaboradores e terceiros, declaram-se comprometidos em proteger todos os ativos ligados à Tecnologia da Informação e Redes de Computadores.

Da Política da Segurança da Informação a Normas e Procedimentos

A Política de Segurança da informação servirá com base na ISO 27000 de base para a criação de outros documentos denominados de Procedimentos e Normas, os quais elencamos e que sempre que surgirem farão com que a Política seja atualizada.

Procedimento de Controle de Acesso a Sistemas e Redes por segregação de função

Procedimento de Criação de Senhas de acesso

Norma para Criação do Grupo de Resposta e Registro de Incidentes Cibernéticos e de Segurança da Informação (Internos ou Externos)

Plano de Continuidade de Negócios

Plano de Recuperação de Desastres

Plano de Treinamento e Divulgação da Política de Segurança da Informação

SEGURANCA FÍSICA

Conjunto de medidas destinadas à proteção e integridade dos ativos da Organização e à continuidade dos seus serviços.

Vulnerabilidades

Devem ser previstos riscos naturais (inundações, tempestades entre outros.), riscos acidentais (incêndios, interrupções de abastecimentos diversos entre outros.), entradas não autorizadas, roubos de patrimônio, entre outros.

Áreas sensíveis

Devem ser mapeadas, levantadas e definida a criticidade de todos os ambientes físicos da organização, principalmente os de alta criticidade, equipamentos, patrimônio físico, recursos humanos, entre outros. Devem ser contemplados acessos físicos a todos os ambientes e o monitoramento dos mesmos, principalmente os considerados de alta criticidade.

SEGURANCA LÓGICA

Conjunto de medidas destinadas à proteção de recursos computacionais contra utilização indevida ou desautorizada, intencional ou não.

Ambiente Lógico

O ambiente operacional, integrado pelos ativos de informação e de processamento será constantemente monitorado pela área de Segurança da Informação. Sendo constatada qualquer irregularidade, o superior responsável será formalmente notificado, devendo tomar as providências cabíveis. A falta de providencias por parte do superior imediato atribui-lhe a responsabilidade solidária advinda do fato.

A administração de rede tem a prerrogativa para desabilitar temporariamente o login e o acesso à Internet de qualquer colaborador, desde que possua indícios de que o mesmo está violando as Normas de Segurança. Neste caso, será gerado um relatório contendo o motivo para o bloqueio da conta. Este relatório será encaminhado a chefia imediata juntamente com os registros comprobatórios.

Vulnerabilidades

Devem estar previstos acidentes por falhas elou sabotagem de hardware, software, aplicativos e procedimentos.

Áreas sensíveis

Sistemas Operacionais, Sistemas Gerenciais de Banco de Dados, Sistemas Gerenciais de Rede, Sistemas Aplicativos e ferramentas de apoio. Devem estar contempladas política de usuários e senhas com definição de perfis de acesso aos ambientes e aplicativos.

SEGURANCA DE TELECOMUNICACÃO

Conceituação

Conjunto de medidas destinadas à proteção das Informações que trafegam por meios eletrônicos ou convencionais e dos recursos utilizados para esse tráfego.

Vulnerabilidades

Devem estar previstos acessos não autorizados às redes de comunicação de dados, adulteração de dados em tráfego, utilização não autorizada de Informações e extravio de formulários ou documentos classificados para não disponibilização pública.

Áreas sensíveis

Redes de comunicação de dados, redes locais, conexões com redes externas, ligações de usuários externos aos servidores da organização, redes IP e telefonia.

CONTINUIDADE DO NEGÓCIO

Conceituação

Conjunto de Planos que contemplam as atividades necessárias para a continuidade dos negócios da Organização, quando houver algum tipo de interrupção nos processos, serviços elou equipamentos considerados críticos.

Vulnerabilidades

Devem estar previstas interrupções significativas das operações essenciais do negócio, causadas pelas vulnerabilidades nas áreas de segurança da informação a serem tratadas.

Áreas sensíveis

Todas as áreas de segurança da informação a serem tratadas.

Comitê de Segurança da Informação

Grupo de gestão multidisciplinar que agrega várias visões corporativas às soluções de segurança. É composto por representantes de diversos departamentos da empresa, com visões isoladas - sob orientação e coordenação direta do Gestor de Segurança da Informação SOC.

Formação:

- Direção de Operações;
- Gerente CGR;
- Gerente NOC
- Gerente Data Center
- Gerente de TI

As principais atribuições do Comitê de Segurança da Informação:

• Revisar as Normas, Procedimentos e Planos;

• Avaliar direcionamento tecnológico para garantir segurança;

• Aprovar as iniciativas para melhoria contínua das medidas de proteção dos bens de Informação da NOVA e de seus clientes;

• Suportar perante a organização as iniciativas da área de Segurança da Informação;

• Este Comitê deve se reunir periodicamente (semestralmente) ou quando convocado pelo Gestor do SOC, extraordinariamente, quando houver necessidade. As reuniões devem possuir como objetivo a avaliação e o aprimoramento da Política de Segurança da Informação, a análise das não-conformidades de Segurança e as ações adotadas para a correção.

Grupo de resposta a incidentes

Grupo formado pelo SOC mais os seguintes representantes das seguintes áreas:

• CGR;

• NOC;

• DATA CENTER;

• Projetos;

- Tecnologia da Informação

Termo de Compromisso com a LGPD e Termo de Confidencialidade.

Termo de Compromisso com a LGPD é o documento da NOVA que compromete colaboradores, terceirizados, prestadores de serviços e parceiros com Lei Geral de Proteção de Dados mantendo as informações de clientes indisponíveis para a finalidade a que o cliente autorizou.

Termo de Confidencialidade é o termo de comprometimento que funcionários e terceiros tem com informações sensíveis da companhia em conformidade com a ISO 27001.

Classificação de Incidentes de Segurança da Informação.

Entende-se como incidente de Segurança, qualquer evento em curso ou ocorrido que contrarie a política de segurança, comprometa a operação do negócio ou cause danos aos ativos da organização.

Propriedade dos softwares aplicativos.

Os sistemas aplicativos e/ou qualquer outro tipo de software, desenvolvidos ou adquiridos pela NOVA FIBRA TELECOM e dessa forma de sua propriedade e utilização devem ficar restritos ao apoio dos negócios da mesma, não sendo permitida sua utilização para fins particulares elou cópias.

Segurança Física

Área de Segurança

A NOVA deve possuir estabelecido seu perímetro físico, identificando todas as suas "fronteiras" e identificados todos os pontos de acesso.

Para as "fronteiras" com prédios vizinhos, devem ser estabelecidos os controles necessários e suficientes, que salvaguardem o acesso às instalações da organização.

As entradas e saídas de cada prédio devem ser dotadas de infraestrutura necessária e suficiente que permita o controle adequado de entrada e saída.

Aplica- se também aos POP´s

Segurança Lógica

Gerenciamento de Tecnologia e Comunicações

a) Sistemas e Software

Todos os sistemas, sejam eles executados em nuvem privada, on-line e/ou misto, estando em Produção, devem possuir documentação atualizada, conforme padrões da metodologia de desenvolvimento de sistemas normatizada e em vigência dos fornecedores de sistemas externos da NOVA.

b) Ambiente de Redes e de Tecnologia da Informação

Todos os equipamentos de infraestrutura, interligações das redes, interligações de hardware de grande porte e softwares básicos e de apoio, devem possuir documentação necessária e suficiente, bem como atualizada, que possibilite entendimento a qualquer técnico capacitado e habilitado, visando manutenções preventivas, corretivas e evolutivas, no ambiente operacional.

Inclui-se todo mapeamento dos POP´s e ranges de IP

c) Gerenciamento e controle de mudanças.

Toda e qualquer mudança no ambiente de produção, seja ela de infraestrutura, hardware, comunicações, softwares básicos, softwares de apoio, sistemas aplicativos, redes LAN e ativos de segurança como firewalls procedimentos entre outros, deve ser executada conforme de **Gestão de Mudanças pelo sistema GESTÃO X**.

d) Gerenciamento e controle de problemas.

Quaisquer problemas que ocorram no ambiente operacional, sejam eles de infraestrutura, hardware, equipamentos de comunicação de dados, softwares e sistemas aplicativos, devem ser registrados com, no mínimo, as seguintes Informações:

• descrição do problema;

• data e hora da ocorrência;

• identificação de quem o registrou e quem foi acionado para solucioná-lo;

• consequências do problema;

• data e hora da solução;

• identificação de quem solucionou;

• descrição da solução adotada.

e) Monitoramento da Segurança

Testes periódicos de vulnerabilidade do ambiente de TI deverão ser realizados com a finalidade de garantir que a implementação de segurança de TI está vigiada e monitorada de forma proativa.

Estes testes incluem as aplicações contratadas, as quais deverão ser solicitadas aos seus fornecedores.

Estes testes podem ser inclusive do tipo PEN TESTS para assegurar que a NOVA está segura quanto as informações próprias e de seus clientes evitando dessa forma paralizações e vazamento de informações conforme a ISO 27000 e Lei Geral de Proteção de Dados - LGPD.

f) Incidentes de Segurança da Informação

Ocorrendo qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança lógica dos ativos da organização os mesmos deverão ser tratados conforme PSI (Política de Segurança ad Informação).

g) Prevenção, Detecção e Correção de Softwares Maliciosos

Medidas para prevenção, detecção e correção de Softwares Maliciosos deverão estar implementadas por toda a organização, para garantir a proteção dos ativos de informação contra softwares maliciosos. O controle dessas medidas deve estar de acordo com a “Matriz de Riscos da NOVA.

h) Segurança de Redes

Assegurar que técnicas e procedimentos de segurança sejam usados para autorizar acessos e controlar as informações que circulam de e para as redes da organização.

i) Segregação de ambientes

A NOVA não possui desenvolvimento de softwares, por isso não possui segregação de ambientes na forma conceitual para esse fim. No entanto para ter aderência a ISO 27000 deve solicitar aos seus fornecedores de aplicação que os mesmos tenham ambiente segregado entre Desenvolvimento, Homologação e Produção e que caso seja necessário usar dados da NOVA para testes que estes sejam mascarados para ter conformidade a ISO 27000 e a LGPD

Procedimentos Operacionais

a) Política de backup

Caberá a área de Tecnologia da Informação definir a Política de Backups e orientar que arquivos salvos em desktops, laptops não são passiveis de ser feitos backup e que em caso de perda as informações não poderão ser recuperadas.

Toda informação importante deverá ser salva nas pastas dos servidores de arquivos disponibilizadas para o departamento.

Segurança e Tratamento de Mídias

Para todas as mídias da NOVA que contenham Informações, sejam elas em meio magnético, ótico ou papel, devem ser observados os seguintes cuidados mínimos:

a) Devem ser guardadas em lugar seguro, diferente do local onde os dados originais estão armazenados, e adequado, de acordo com as especificações do fabricante da mídia.

b) As mídias que forem transitar para fora das instalações de sua origem devem ter a sua saída registrada e a garantia de sua chegada ao destino, também registrada. Além disso, devem ser embaladas, acondicionadas e transportadas de forma adequada, para garantir sua integridade.

c) As mídias em meio magnético ou ótico devem ser identificadas externamente, quanto ao seu conteúdo, indicando, quando necessário, o prazo de retenção e observações sobre a mesma.

d) Quando forem descartadas, devem ser apagadas elou destruídas de forma completa e total, através de trituração ou incineração.

Controle de Acesso aos Recursos Computacionais

A NOVA poderá a título de assegurar o correto uso dos recursos computacionais e ou de rede monitorar seu uso, evitando uso de sites, aplicações, streamers que indiquem mau uso de ferramentas, como de cunho que seja ofensivo a raça, credo ou orientação sexual.

Identificação e autenticação de usuários

• O usuário somente deve possuir acesso ao ambiente computacional através de uma identificação de acesso e uma senha;

• A identificação de acesso do usuário deve ser única, pessoal e intransferível;

• A senha associada à identificação de acesso deve ser secreta e de conhecimento exclusivo do usuário para o qual foi custodiada;

• A senha não pode ser divulgada a terceiros, devendo-se evitar o uso de combinação simples ou óbvia na sua criação;

Observação Importante sobre o uso de chaves genéricas – Caso de necessidade de uso de identificação genérica, ou seja, chaves genéricas as mesmas deverão obedecer ao procedimento especifico para tratamento destas com justificativa especial e apenas para sistemas internos. Para sistemas de uso externo a NOVA o procedimento não se aplica.

1) ENTENDE-SE COMO CHAVE GENÉRICA O USUÁRIO QUE NÃO IDENTIFICA UM ÚNICO USÚARIO, MAS UM GRUPO. PARA CONTROLE DESTES ACESSOS LOGS ADICIONAIS SERÃO IMPLEMENTADOS IDENTIFICANDO QUAL USUARIO UTILIZOU EFETIVAMENTE A CHAVE/LOGIN DE ACESSO.
2) O USO DESSAS CHAVES DEVER TER AUTORIZAÇÃO DO GESTOR RESPONSÁVEL PELA AREA

Uso das Estações de Trabalho, laptops, tablets, smatphones e outros

Os computadores e sistemas de comunicações não devem ser utilizados para fins pessoais. Os recursos computacionais, colocados à disposição do colaborador deverão estar inventariados corretamente no departamento de atividade do colaborador e o respectivo Termo de Responsabilidade assinado por este. Na ausência deste registro, o superior imediato assume esta responsabilidade. Todo o colaborador, indicado no Termo de Responsabilidade ou a chefia imediata, na ausência de indicação, responde pelo mau uso ou dano causado nos equipamentos.

Compartilhamento de Recursos

O compartilhamento de diretórios e/ou arquivos nas estações de trabalho e notebooks deve ser atribuído única e exclusivamente para facilitar e/ou agilizar o trabalho das atividades laborais, não devendo ocorrer em qualquer outra situação.

Arquivos Multimídias

De maneira geral o uso de mídias e portas USB é proibido no ambiente da NOVA. Liberações podem existir de acordo com a necessidade e avaliação dos Gestores.

Os colaboradores que são autorizados a utilizar mídias e portas USB assumem a responsabilidade de utilizar os acessos de forma ética e apenas para o exercício da função.

Regras para criação de logins e senhas – Ver Procedimento de criação de logins e senhas

• Para serem criados logins e senhas, deve-se ter uma solicitação da área de custódia do novo usuário, contendo, pelo menos, o nome completo do usuário, o local de trabalho e a data de início de utilização do login;

• Periodicamente, a cada 6 meses, deve ser enviada para os Gestores, uma relação dos usuários que tiveram seu login, senha e perfil de acesso autorizado por eles. Os Gestores devem confirmar a Informação, alterá-la caso seja necessário ou revogar o login;

• Os colaboradores são responsáveis por toda atividade realizada com sua conta. As contas de colaboradores não podem ser utilizadas por outras pessoas que não sejam os colaboradores para os quais elas foram geradas. Exceções como uso de chaves compartilhadas podem ser tratadas pelo gestor da área.

As senhas de acesso são de uso individual e restrito. O compartilhamento das senhas e terminantemente proibido, pois expõe o colaborador à responsabilidade pelas ações que outras pessoas realizarão com sua senha de acesso. Caso ocorra tal compartilhamento, seja de natureza autorizada ou não, o colaborador possuidor da senha compromissada assumira todas as responsabilidades e consequências das ações realizadas.

Perfil de acesso dos usuários

• Cada usuário deve possuir um perfil de acesso à rede de dados que deve indicar os diretórios, grupos, aplicativos, funcionalidades e suas permissões de direito;

• Aos sistemas, cada usuário deve possuir os perfis necessários para o desempenho de suas funções;

• Sempre que necessário, deve ser estabelecido o mesmo perfil de acesso para um grupo de usuários;

• Estes perfis devem estar normatizados;

• A permissão de acesso aos ativos de informação da organização deve ser solicitada formalmente conforme procedimento para liberação de acesso lógico, isto é, por abertura de chamado.

Responsabilidades

As responsabilidades referentes ao controle de acesso aos recursos computacionais são classificadas conforme descrição abaixo:

I. Proprietário das Informações

Pessoa que utiliza os recursos de Tecnologia da Informação de propriedade ou sobre custódia da NOVA para a geração de informação de qualquer natureza.

Autoridade e a responsabilidade do proprietário das Informações:

• Delegar responsabilidade e atribuições ao depositário das Informações;

• Classificar os bens de Informação, de acordo com sua natureza crítica e sigilosa;

• Estabelecer as regras de proteção dos bens de Informação, quanto aos acessos, backups entre outros.;

• Monitorar o cumprimento das regras estabelecidas;

• Responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não-conformidade;

• Notificar não-conformidades de Segurança ao Gestor imediato e ao Gerente de Segurança da Informação.

USB

II. Custodiante

A Gestão de Tecnologia da Informação é a responsável pelo processamento, armazenamento e custódia das Informações.

Autoridade e responsabilidade do (a) Custodiante:

• Administrar os controles estabelecidos pelo proprietário da aplicação e de seus dados;

• Administrar o acesso aos recursos do sistema de processamento e prover procedimentos de Segurança;

• Controlar o acesso à Informação;

• Providenciar a proteção física;

• Simular e executar os planos de continuidade;

• Resolver as não-conformidades de Segurança.

III. Usuário da Informação

E todo colaborador, prestador de serviço, terceirizado, parceiro, estagiário ou fornecedor, que tenha acesso aos bens de Informação da NOVA.

É vedado a utilização pelo funcionário dos recursos tecnológicos da organização para fins pessoais. Ocorrendo eventual extravio de informações e/ou dados, a NOVA não poderá ser responsabilizada.

Autoridade e responsabilidade do usuário da Informação:

• Zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação pessoal de acesso;

• Respeitar e preservar o grau de confidencialidade da Informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;

• Utilizar os recursos tecnológicos (equipamento, programas e sistemas) e as Informações somente para desempenho das suas atividades profissionais e dentro dos padrões de utilização descritos na Política de Segurança da Informação, sendo assim vedado o seu uso para fins pessoais;

• Assinar o Termo de Responsabilidade e Sigilo onde são estabelecidas as regras sobre o uso dos bens de Informação;

• Solicitar autorização ao superior imediato, quando necessário, para utilização de funcionalidades que estejam fora dos padrões pré-determinados na Política de Segurança da Informação;

• Notificar de imediato as não-conformidades de Segurança ao Gestor imediato e ao Gestor de Segurança da Informação.

IV. Gestor de área (Coordenador e Gestor)

• Gerenciar o cumprimento da Política de Segurança, por parte dos colaboradores sob sua gestão;

• Identificar e comunicar a quem de direito os desvios praticados e adotar as medidas corretivas apropriadas;

• Não permitir o acesso dos colaboradores demitidos ou demissionários aos ativos de informações sob sua responsabilidade;

• Proteger, em nível físico e lógico, os ativos de informação sob sua responsabilidade;

• Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a informação da empresa;

• Comunicar formalmente à Gerência de Tecnologia da Informação, qual o perfil de acesso dos colaboradores a ele subordinados;

• Comunicar formalmente à Gerência de Tecnologia da Informação, quais os colaboradores demitidos ou transferidos, para exclusão no cadastro dos usuários;

• Dar conhecimento aos responsáveis pela segurança da ocorrência de qualquer irregularidade ou desvio das Políticas de segurança, estando a ele correlacionada ou não.

V. Colaboradores: Redes Sociais

• Cumprir integralmente a Política de Segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

• Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

• Utilizar os Sistemas de Informações e os recursos a ela relacionados somente para a execução das atividades correlacionadas com o desempenho de seu trabalho;

• Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;

• Manter o caráter sigiloso da senha de acesso aos recursos e sistemas da empresa;

• Não compartilhar, sob qualquer forma, informações sigilosas com outros que não tenham a devida autorização de acesso;

• Responder, por todo e qualquer acesso, aos recursos da empresa bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;

• Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;

• Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio da Política de Segurança da empresa;

Camadas De Segurança

Para a devida proteção do ambiente, devem ser projetadas 4 (quatro) camadas de acesso:

• **Acesso ao ambiente;**

• **Acesso aos sistemas aplicativos;**

• **Acesso às funções dos sistemas aplicativos;**

• **Acesso aos dados**.

Sempre que possível o login e a senha de acesso devem ser únicos para todas as camadas de Segurança.

Devem ser exibidos para os usuários apenas os arquivos, os softwares e as funcionalidades a que eles têm direito de acesso, ficando sob responsabilidade do mesmo informar ao seu superior sobre acessos disponibilizados em demasia.

Trilhas de Auditoria

Recomenda-se a existência de softwares de Segurança, e que estes mantenham registros sobre os acessos dos usuários, indicando, sempre que possível, o arquivo, o software, a data e hora que foram acessados.

Computação Móvel e Trabalho Remoto.

Sempre que necessário e viável, a NOVA deve disponibilizar sistemas na Internet, através de sua Gestão de Tecnologia da Informação ou de fornecedores parceiros. Para que os acessos realizados a estes sistemas sejam feitos com segurança, devem ser previstos e adotados mecanismos visando a proteção dos bens de Informação, tais como Certificação digital, Softwares de Segurança, Antivírus, Firewalls corporativos e individuais, Criptografia e entre outros.

É vedado ao colaborador, prestador de serviços, terceiros ou fornecedores, acesso ao ambiente da Companhia com equipamentos de computação pessoal, salvo com autorização formal do seu Gestor, do Gestor do SOC e do Gestor de TI.

Trânsito de Informações

O trânsito de Informações deve ser feito por um caminho ou meio confiável com controles que ofereçam autenticidade do conteúdo, proteção de submissão e recebimento e não repúdio da origem. Os procedimentos acima citados contemplam e padronizam a geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, entrada, uso e arquivamento de chaves criptográficas para garantir a proteção das chaves contra modificação e acessos não autorizados.

Administração de Acessos

A NOVA através da gerencia de ferramenta de Active Directory (AD) pode utilizar os mecanismos que permitem registros de acessos aos ambientes, indicando, minimamente e sempre que possível, os recursos acessados, quem efetuou o acesso, data e hora, tentativas de acesso com senhas erradas, tentativas de acesso de estações de trabalho não permitidas, tentativas de acesso em horários não permitidos entre outros.

É realizado o monitoramento e gerenciamento dos acessos, pela Gestão de Segurança SOC e por auditores que porventura sejam requisitados.

Acesso à Internet, Canais de Comunicação, correio eletrônico, telefone e mensagens instantâneas.

a) Internet

O acesso à Internet corporativa deve ser restrito às atividades profissionais.

São utilizados mecanismos de monitoramento que permitem o gerenciamento do uso desse recurso e que os mesmos são regidos conforme Leis vigentes no País.

Bloqueio e controle de Sites na Internet

Os sistemas da empresa são configurados rotineiramente para evitar que os colaboradores se conectem em sites não relacionados as atividades da empresa. Os colaboradores que usam os sistemas de informações não têm permissão para acessar um site cujo conteúdo seja de explicitação sexual, racista ou outro material potencialmente ofensivo. A capacidade para conectar-se a um site específico não implica em permissão para acessar o mesmo.

O acesso de qualquer computador da rede da empresa à Internet deverá ser feito exclusivamente através de equipamentos de controle (Firewall e Proxy) corporativos. Outras formas de acessar à Internet, como conexões dial-up através de um provedor externo ou cascateamento de proxies, visando burlar as barreiras corporativas, são terminantemente proibidas de serem empregadas. Os usos dessas ferramentas são autorizados pelo Gestor apenas para realização do trabalho, conforme procedimentos operacionais. (Procedimento de USO DE RECURSOS COMPUTACIONAIS E DE ACESSOS A MIDIAS, USB, SITES E SOCIAL MEDIA)

Redes Sociais, Grupos de discussão, salas de conversação

A não ser que seja autorizado pela gerência responsável, os colaboradores não devem participar de grupos de discussão na Internet, salas de conversação e redes sociais, bem como outros fóruns públicos eletrônicos, **quando utilizando recursos da empresa**. O uso dessas ferramentas, sites e aplicações são autorizadas apenas para realização do trabalho.

Obs. - O uso de ferramentas de conversação ou reuniões com ambientes externos é permitido quando se tratar de assuntos de trabalho, como por exemplo reunião com fornecedores, audiências, participação em seminários e etc.

(Ver Procedimento de USO DE RECURSOS COMPUTACIONAIS E DE ACESSOS A MIDIAS, USB, SITES E SOCIAL MEDIA)

Correio eletrônico

O endereço de correio eletrônico fornecido pela NOVA para cada colaborador, prestador de serviço ou terceiro será utilizado única e exclusivamente para atividades relacionadas ao trabalho na organização.

Ao final do e-mail a seguinte mensagem deverá ser exibida:

"Aviso de Confidencialidade: Esta comunicação deve ser lida apenas pelo seu destinatário e não pode ser retransmitida sem autorização formal. Caso seja recebida indevidamente, por favor destrua-a. Qualquer reprodução, alteração, distribuição e/ou publicação é estritamente proibida.

Notice of Confidentiality: This document should only be read by those persons to whom it is addressed and can not be relayed without formal permission. If you have received this e-mail message in error, please destroy it. Any form of reproduction, modification, distribution and./or publication of this e-mail message is strictly prohibited. "

Correio eletrônico como comunicação pública

Os colaboradores devem evitar enviar números de cartões de crédito, senhas, informações de pesquisas e desenvolvimento, informações de clientes e outros dados sensíveis via correio eletrônico. A empresa não se responsabiliza pelas informações pessoais, fornecidas pelos seus colaboradores através da Internet ou qualquer outra rede pública, que de alguma maneira venha a ser manipulada elou utilizada por terceiros.

O sistema de correio eletrônico é disponibilizado para ser usado nas atividades da empresa, e somente seu uso profissional está autorizado. E proibido o uso de correio eletrônico externo

através da utilização da infraestrutura de comunicações da empresa. Tal proibição leva em consideração principalmente a grande quantidade de códigos maliciosos, vírus, cavalos de Tróia, worms e exploits oriundos dos provedores externos.

NOTA IMPORTANTE DE INFORMAÇÃO LEGAL.

Restrições do conteúdo das mensagens

Os colaboradores estão proibidos de enviarem ou encaminharem quaisquer mensagens via os sistemas de informações da empresa, que possa ser considerada como difamatória, inoportuna ou de natureza explicitamente sexual.

Os colaboradores também são proibidos de enviarem ou encaminharem mensagens ou imagens que possam ter conotação ofensiva de raça, sexo, nacionalidade, religião, filiação política, deficiência física, entre outros.

Filtros de Conteúdo

Com a finalidade de minimizar a contaminação por vírus, otimizar o tráfego de rede e o espaço de armazenamento em disco no servidor de correio eletrônico, são filtradas de forma automática as mensagens que possuam arquivos anexados com as seguintes extensões: JPG, JPEG, MP3, BAT, EXE, COM, INI, PIF, AVI, MPEG, BMP, GIF, PPT e PPS. Podem e devem ser adicionadas a esta lista, sem aviso prévio, qualquer outra extensão que a Gestão de Tecnologia da Informação julgue conveniente.

Telefones

A utilização dos telefones da organização é restrita ao desempenho das atividades laborais dos colaboradores.

Continuidade dos Negócios

Visando garantir a continuidade dos negócios da NOVA um “Planos de Continuidade de Negócio” será elaborado e revisado PERIODICAMENTE pelas Gerencias da DIRETORIA DE OPERAÇÕES. Este Plano de Continuidade de Negócio deverá ser elaborado somente para os ativos considerados críticos e que sejam aprovados pela DIRETORIA DE OPERAÇÕES.

Condutas Gerais

As Políticas de conduta gerais abordadas abaixo, são implantadas na NOVAS, através dessa Política de Segurança da Informação, conforme descritos abaixo.

a) Materiais sobre a mesa de trabalho

• Recomenda-se que Informações impressas que sejam sensíveis ou sigilosas não devem ser mantidas sobre a mesa de trabalho;

• Não anotar informações sensíveis explicitas em qualquer objeto em exposição,

• Não deixar pen drive, cd ou dvd conectados ao computador ou outros dispositivos de midia;

b) Bloqueio de Tela do computador

• Computadores e impressoras quando utilizados devem ser bloqueados quando na ausência do usuário responsável;

• Nos computadores, utilizar um protetor de tela que solicite uma senha para acesso;

Documentação física

a) Armazenamento seguro

As informações críticas do negócio devem ser guardadas em lugar seguro quando não em uso, principalmente quando o escritório está desocupado.

b) Cuidados com impressão

Caso seja necessária impressão, documentos com informações sensíveis devem ser recolhidos imediatamente, a fim de impedir que uma pessoa não autorizada tenha acesso à informação.

Pontos de entrada e saída de correspondência devem ser protegidos e monitorados.

c) Cuidados com o Lixo

Todo lixo que contenha informação sensível deve ser eliminado através de “Máquina picotadora” ou similar quando esta existir, ou destruição manual (rasgando). Sempre se certifique que o descarte ocorreu de maneira correta e que impossibilita qualquer tentativa de reconstrução.

Conduta em ambiente externo:

- Cuidado com exposição das informações sensíveis em relação a empresa.

Sanções

Aos colaboradores e terceiros que, de forma intencional ou não infringirem **a LEI GERAL DE PROTEÇÃO DE DADOS**, estarão sujeitos a possíveis sanções estipuladas no ordenamento jurídico brasileiro.