

The cover features a dark teal background with a large, dark grey rectangular panel in the center. The panel is flanked by vertical bands of a repeating geometric pattern consisting of interlocking circles and semi-circles. The title is printed in white, uppercase letters on the central panel.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO FUNDAJ

**VERSÃO REVISADA DIA
16112021**

Sumário

| | |
|---|----|
| POLÍTICA DE SEGURANÇA DA INFORMAÇÃO..... | 5 |
| OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO | 5 |
| MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO | 5 |
| RESPONSABILIDADE DOS SERVIDORES E COLABORADORES DA FUNDAJ | 5 |
| CLASSIFICAÇÃO DA INFORMAÇÃO | 6 |
| DADOS DOS FUNCIONÁRIOS..... | 6 |
| ADMISSÃO E DESLIGAMENTO DE SERVIDORES / TERCEIRIZADOS / ESTAGIÁRIOS E BOLSISTAS..... | 7 |
| TRANSFERÊNCIA DE SERVIDOR / TERCEIRIZADO / ESTAGIÁRIOS..... | 7 |
| PROGRAMAS ILEGAIS..... | 7 |
| PERMISSÕES E SENHAS..... | 8 |
| COMPARTILHAMENTO DE DADOS..... | 9 |
| BACKUP (CÓPIA DE SEGURANÇA DOS DADOS)..... | 9 |
| CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS..... | 9 |
| SEGURANÇA E INTEGRIDADE DOS DADOS..... | 10 |
| PROPRIEDADE INTELECTUAL..... | 10 |
| ACESSOS A INTERNET..... | 10 |
| USO DO CORREIO ELETRÔNICO (E-MAIL)..... | 11 |
| NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS..... | 11 |
| USO DE NOTEBOOKS (COMPUTADORES PESSOAIS) NA FUNDAJ..... | 12 |

Sumário

| | |
|--|----|
| RESPONSABILIDADE DOS DIRETORES /COORDENADORES/ GERAIS COORDENADORES / CHEFE DE DIVISÃO/CHEFE DE SERVIÇO..... | 12 |
| SISTEMAS DE TELECOMUNICAÇÕES | 13 |
| USO DE ANTIVÍRUS..... | 13 |
| PENALIDADES..... | 13 |



REPÚBLICA FEDERATIVA DO BRASIL

MINISTÉRIO DA EDUCAÇÃO | MEC

FUNDAÇÃO JOAQUIM NABUCO | FUNDAJ

COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO | CTINFO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de segurança da informação, na FUNDAJ, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Fundaj, ou acesso a informações pertencentes à FUNDAJ. Todo e qualquer usuário de recursos computadorizados da Fundaj tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

Exponha a Fundaj a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.

Envolve a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

Envolve o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização da missão da FUNDAJ.

MISSÃO DO SETOR DE TECNOLOGIA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização da missão da FUNDAJ. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

RESPONSABILIDADE DOS SERVIDORES E COLABORADORES DA FUNDAJ

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização da missão da FUNDAJ. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Diretor/Coordenador/Chefe de Divisão/Chefe de Serviço de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

- 1 – Pública
- 2 – Interna
- 3 – Confidencial
- 4 – Restrita

Conceitos:

- **Informação Pública:** É toda informação que pode ser acessada por usuários da Fundação Joaquim Nabuco, clientes, fornecedores, prestadores de serviços e público em geral.
- **Informação Interna:** É toda informação que só pode ser acessada por funcionários da Fundação Joaquim Nabuco. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da Fundação Joaquim Nabuco.
- **Informação Confidencial:** É toda informação que pode ser acessada por usuários da Fundação Joaquim Nabuco e por parceiros da Fundação Joaquim Nabuco. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da Fundação Joaquim Nabuco.
- **Informação Restrita:** É toda informação que pode ser acessada somente por usuários da Fundação Joaquim Nabuco explicitamente indicado pelo nome ou por área a que pertence.

A divulgação não autorizada dessa informação pode causar sérios danos à instituição ou comprometer a estratégia da Fundação Joaquim Nabuco. Todos os Diretores/Coordenadores/Chefes de Divisão/Chefes de Serviço devem orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

DADOS DOS FUNCIONÁRIOS

A FUNDAJ se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução de sua missão. Todos os Dados Pessoais de Funcionários que porventura sejam armazenados, serão considerados dados confidenciais. Dados Pessoais de Funcionários sob a responsabilidade da FUNDAJ não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pela nossa instituição e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da FUNDAJ. Por outro lado, os funcionários comprometem a não armazenar dados pessoais nas instalações da FUNDAJ, sem prévia e expressa autorização por parte da diretoria.

ADMISSÃO E DESLIGAMENTO DE SERVIDORES / TERCEIRIZADOS / ESTAGIÁRIOS E BOLSISTAS

O RH da Fundaj deverá informar a Coordenação de TI, toda e qualquer movimentação de Terceirizados ou estagiários, e admissão/desligamento de servidores, para que os mesmos possam ser cadastrados ou excluídos nos sistemas da Fundaj. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pela coordenação de TI.

Cabe ao setor solicitante da contratação a comunicação a Coordenação de TI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de Terceirizados ou estagiários deverá também ser informado o tempo em que o mesmo encontra-se trabalhando na Fundaj para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão/desligamento/aposentadoria, a Coordenação Geral de Planejamento e Gestão de Pessoas deverá comunicar o fato o mais rapidamente possível à Coordenação de TI, para que o funcionário demitido seja excluído do sistema.

Cabe a Coordenação Geral de Planejamento e Gestão de Pessoas dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da FUNDAJ. Nenhum Servidor, estagiário ou terceirizado, poderá ser contratado, sem ter expressamente concordado com esta política.

TRANSFERÊNCIA DE SERVIDORES/ TERCEIRIZADOS / ESTAGIÁRIOS

Quando um servidor for promovido ou transferido do nível ou coordenação, deverá comunicar o fato à Coordenação de TI, para que sejam feitas as adequações necessárias para o acesso do referido Servidor ao sistema informatizado da Fundaj.

PROGRAMAS ILEGAIS

FUNDAJ respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da FUNDAJ. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na FUNDAJ.

Os usuários não podem, em hipótese alguma, instalar este tipo de “software” (programa) nos equipamentos da Fundaj mesmo porque somente o pessoal da Coordenação de TI tem autorização para instalação de programas previamente autorizados dentro da Política de Segurança da Fundação. Periodicamente, a Coordenação de TI fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a Fundaj por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos as sanções previstas neste documento.

PERMISSÕES E SENHAS

Todo usuário para acessar os dados da rede da FUNDAJ, devesse possuir um login e senha previamente cadastrados pelo Coordenação de TI.

Quem deve fornecer os dados referentes aos direitos do usuário é o responsável direto pela sua chefia, que deve preencher uma ficha e entregá-la a de Coordenação Geral de Planejamento e Gestão de Pessoas. Quando da necessidade de cadastramento de um novo usuário para utilização da “rede”, sistemas ou equipamentos de informática da Fundaj, o setor de origem do novo usuário deverá comunicar esta necessidade a Coordenação de TI, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

Coordenação de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 45 (quarenta e cinco) dias. Por segurança, a Coordenação de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc) deverão comunicar a Coordenação de TI qual será o seu substituto quando de sua ausência da FUNDAJ, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pela Coordenação de TI.

COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de pastas nos computadores e desktops da FUNDAJ. Todos os dados deverão ser armazenados nos Servidores da rede, e a autorização para acessá-los deverá ser fornecida pelo Servidor AD (Active Directory). O Pessoal de TI está orientado a periodicamente verificar todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados fora dos servidores.

Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso do AD. Não são permitidos na FUNDAJ o compartilhamento de dispositivos móveis tais como pen-drivers e outros.

BACKUP (CÓPIA DE SEGURANÇA DOS DADOS)

Todos os dados da FUNDAJ deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do Setor Interno de TI e deverão ser feitas diariamente. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado.

As copias deverão abranger todos os dados da FUNDAJ, que deverão estar nos servidores. As copias deverão ser protegidas por senhas para evitar que pessoas não autorizadas tenham acesso a estes dados em caso de perda ou roubo da mídia.

CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

Não é política da FUNDAJ o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede. Nestes e em outros casos, o pessoal de TI deverá alertar ao usuário que ele deve fazer backup dos dados de sua máquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da FUNDAJ.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da FUNDAJ a Coordenação de TI disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

SEGURANÇA E INTEGRIDADE DOS DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva da Coordenação de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

PROPRIEDADE INTELECTUAL

É de propriedade da FUNDAJ, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a FUNDAJ.

ACESSOS À INTERNET

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na FUNDAJ. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pela Coordenação de TI, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos Servidores que terão permissão para uso (navegação) da Internet é atribuição da Direção da Fundaj, com base em recomendação do Coordenador de TI. Não é permitido instalar programas provenientes da Internet nos microcomputadores da FUNDAJ, sem expressa anuência da Coordenação de TI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos assuntos da FUNDAJ;
- Que promovam discussão pública sobre os assuntos da FUNDAJ, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

USO DO CORREIO ELETRÔNICO(E-MAIL)

O correio eletrônico fornecido pela FUNDAJ é um instrumento de comunicação interna e externa para a realização das operações da FUNDAJ. As mensagens devem ser escritas em linguagem formal não devem comprometer a imagem da FUNDAJ, não podem ser contrárias à legislação vigente e nem aos princípios éticos da FUNDAJ.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da Fundação;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da FUNDAJ.

Para incluir um novo usuário no correio eletrônico, a respectiva Coordenação deverá fazer um pedido formal ao RH, e o mesmo repassará a Coordenação de TI, que providenciará a inclusão do mesmo. A utilização do “e-mail” deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico a Coordenação de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mail gratuito (liberados em alguns sites da web), nos computadores da FUNDAJ. A Coordenação de TI poderá, visando evitar a entrada de vírus na FUNDAJ, bloquear o recebimento de e-mails provenientes de sites gratuitos.

NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

A Coordenação de TI é responsável pela aplicação da Política da FUNDAJ em relação a definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas (“softwares”) ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pela Coordenação de TI. Não é permitido a compra ou o desenvolvimento de “softwares” ou “hardwares” diretamente pelos usuários, exceto mediante autorização da DIPLAD.

USO DE NOTEBOOKS (COMPUTADORES PESSOAIS) NA FUNDAJ

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da FUNDAJ, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
- O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:
 - Fora do trabalho:
 - Mantenha o equipamento sempre com você;
 - Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
 - Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
 - Atenção ao transportar o equipamento na rua.
 - Em caso de furto
 - Registre a ocorrência em uma delegacia de polícia;
 - Comunique ao seu superior imediato e a Coordenação de TI;
 - Envie uma cópia da ocorrência para a Coordenação de TI.

RESPONSABILIDADES DOS DIRETORES/COORDENADORES/CHEFES DE DIVISÃO/CHEFES DE SERVIÇO

Os Diretores, Coordenadores e Chefe de divisão são responsáveis pelas definições dos direitos de acesso do seus servidores aos sistemas e informações da Fundaj, cabendo a eles verificar se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

A Coordenação de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinado usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da FUNDAJ, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade das coordenações, de acordo com as definições da Diretoria da FUNDAJ.

USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa à FUNDAJ deve ser verificado por programa antivírus (Antivírus padrão da Fundaj é o Microsoft, incluso na Segurança do Windows). Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

José Ferreira Rodrigues
Coordenador de Tecnologia da Informação
Mat. SIAPE nº 3156536