PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPESESP

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Introdução

A informação é um ativo de grande valor para as organizações, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante da CAPESESP, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.

Por princípio, a segurança da informação deve abranger três conceitos básicos: confidencialidade, integridade e disponibilidade. Para assegurar esses três conceitos, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, perda, acidentes e outras ameaças.

A Política de Segurança da Informação depende da combinação de diversos elementos, dentre eles, o comprometimento de dirigentes, empregados e colaboradores.

Objetivo

Este documento aborda as Diretrizes, Normas, Procedimentos, Guias e Padrões estabelecidos para gerenciamento da segurança das informações da CAPESESP, tendo como referência a norma ABNT NBR ISO/IEC 27001:2006, o modelo COBIT 4.1, processo DS5 e a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Esta política constitui um compromisso formal da CAPESESP e de seus profissionais com a proteção das informações sob sua guarda, colaborando para que as fontes de informação sejam utilizadas dentro do respeito e da ética, fazendo o uso apropriado e responsável dos recursos computacionais para os objetivos da empresa, sem colocar em risco os ativos e bens de informação da CAPESESP.

Esta política garante a aderência dos usuários de recursos de Tecnologia da Informação – TI ao Código de Ética e de Padrões de Conduta Profissional da CAPESESP.

Campo de Aplicação

As orientações contidas neste documento são aplicáveis de forma geral a todos os usuários que manuseiam ou acessam bens ou ativos de informação da CAPESESP.

A direção da CAPESESP está comprometida em proteger todos os bens ou ativos ligados à TI, sendo responsável por cumprir e fazer cumprir esta Política e assegurar que suas equipes possuam acesso e conhecimento das Normas e dos Procedimentos de Segurança da Informação.

DAS RESPONSABILIDADES ESPECÍFICAS

DA DIRETORIA-EXECUTIVA

Aprovar a Política de Segurança da Informação e determinar a adoção de medidas necessárias para o seu cumprimento.

Assegurar que as equipes tenham pleno conhecimento dessa Política e fazer cumprir todas as normas constantes neste documento.

Tomar as decisões administrativas cabíveis sobre os casos de violação desta Política e tratar as exceções, ponderando os benefícios e os riscos à operação da CAPESESP, os requisitos que a originaram, bem como as condições e os períodos das exceções.

DOS GESTORES DE PESSOAS E/OU PROCESSOS

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Antes de conceder acesso às informações da instituição, exigir a assinatura de um **Acordo de Confidencialidade** dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, os procedimentos e os sistemas sob sua responsabilidade para atender a esta PSI.

DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Desempenhar atividades de monitoração e controle de segurança da informação, previstas nas normas e procedimentos desta Política.

Aferir o nível de segurança dos sistemas e ambientes em que circulam as informações da CAPESESP.

Analisar riscos e vulnerabilidades e propor projetos e iniciativas à DADM, relacionados à melhoria da segurança da informação da CAPESESP.

Comunicar à DADM as não conformidades apuradas nos processos de auditoria e monitoramento de segurança.

Configurar os equipamentos, instalar os softwares e garantir as atualizações de segurança.

Administrar, proteger e testar as cópias de segurança dos sistemas e dados da CAPESESP.

DA DIVISÃO DE RECURSOS HUMANOS

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da CAPESESP.

Exigir dos colaboradores a assinatura do **Termo de Compromisso e Ciência**, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade sobre todos os ativos de informações da CAPESESP, mesmo após a perda do vínculo com a entidade.

Informar prontamente à DSO todos os desligamentos, afastamentos e quaisquer modificações no quadro de pessoal da CAPESESP.

DOS COLABORADORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto nesta Política de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que a recebeu não estiver cumprindo as condições definidas no contrato.

DOS COLABORADORES EM GERAL

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à CAPESESP e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Classificação da Informação

É responsabilidade de cada gestor de área classificar a confidencialidade da informação que está sob sua guarda, seguindo os critérios abaixo:

- **Pública** – Informação com linguagem e formato dedicado ao público em geral. Exemplos: campanha de marketing externo, demonstrações contábeis públicas, informações do site etc.

- **Uso Interno** – Informação de uso exclusivo dos empregados da CAPESESP. Exemplos: correspondências internas, portarias, políticas corporativas etc.

- **Confidencial** – Informação reservada, sem autorização para divulgação. Exemplos: atas de reunião da Diretoria -Executiva e dos Conselhos Deliberativo e Fiscal, relatórios da Comissão de Ética, processos jurídicos, informações contábeis não divulgadas, contratos com fornecedores e rede de atendimento, informações pessoais de colaboradores e beneficiários etc.

É importante que as informações classificadas como Uso Interno e Confidencial tenham tratamento diferenciado e sua guarda possibilite a garantia do seu nível de confidencialidade.

Comportamento Seguro e Uso Responsável da Informação

É crucial a adoção de comportamento seguro e uso responsável, visando à integridade e proteção das informações da entidade, pautados pelas atitudes e/ou orientações a seguir:

- Fazer uso apropriado dos ativos de informação da CAPESESP, cumprindo esta Política, respeitando a ética, o bom senso, a razoabilidade, os princípios estabelecidos nos valores corporativos e de forma consistente com os objetivos da entidade. As ações em desacordo com estas orientações são consideradas inapropriadas e passíveis de sanção de acordo com o Código de Ética e de Padrões de Conduta profissional da CAPESESP;

- Adotar atitude proativa e engajada visando à proteção das informações contra divulgação, alteração, destruição ou acesso não autorizados pela CAPESESP;

- Informações confidenciais da CAPESESP não podem ser transportadas em qualquer meio (CD, DVD, *pendrive,* papel, etc), sem as devidas autorizações e proteções.

- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, reveladas ou divulgadas a terceiros (inclusive colaboradores da própria empresa), tampouco anotadas em papel ou em sistema visível ou de acesso não protegido.

- Somente softwares homologados pela CAPESESP podem ser instalados nas estações de trabalho, o que deve ser feito, exclusivamente, pela equipe da DSO.

- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados.

- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos durante sua vida útil e, posteriormente, devidamente destruídos ou descartados.

- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas normas deve ser esclarecida com a DSO ou a DADM.

Segurança do Ambiente Físico

É vedado o acesso à área física do datacenter da CAPESESP, sem autorização prévia da DSO.

É obrigatório o uso do crachá de identificação, em local visível, por todos os empregados, dentro das áreas internas da CAPESESP.

O acesso de visitantes às áreas internas da CAPESESP deverá ser previamente autorizado pela DADM e supervisionado pelo gestor da área que será visitada.

Não é permitido aos colaboradores e visitantes tirar fotos, gravar, filmar e/ou publicar imagens dos ambientes internos da CAPESESP que comprometam a segurança, o sigilo das informações ou a imagem da empresa e de outros empregados.

Correio Eletrônico Corporativo

O correio eletrônico da CAPESESP (@capesesp.com.br) deve ser utilizado para fins corporativos e relacionados às atividades do colaborador dentro da instituição. A utilização desse serviço para fins pessoais é permitida, desde que feita com bom senso e não prejudique a entidade ou cause impacto no tráfego da rede.

Todo empregado da CAPESESP receberá uma conta de e-mail, com acesso exclusivo, do tipo **nome.sobrenome@capesesp.com.br**.

Os colaboradores terceirizados receberão uma conta de e-mail do tipo **nome.sobrenome.empresa@capesesp.com.br**.

Cada conta de e-mail tem a capacidade de armazenamento de 50 GB. Cabe ao usuário administrar o conteúdo de sua caixa postal, de forma que não ultrapasse o tamanho máximo permitido.

É proibido aos colaboradores o uso do correio eletrônico da CAPESESP para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição e com autorização prévia da DADM;

- expedir mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- encaminhar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a CAPESESP vulneráveis a ações civis ou criminais;

- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar quaisquer punições;

- produzir, transmitir ou divulgar mensagem que:

  - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da CAPESESP;

  - apresente ameaças eletrônicas, como spam, mail bombing ou vírus de computador;

  - possua arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

  - vise obter acesso não autorizado a outro computador, servidor ou rede;

  - intencione interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

  - intente burlar qualquer sistema de segurança;

  - objetive vigiar secretamente ou assediar outro usuário;

  - aspire acessar informações confidenciais sem explícita autorização do proprietário;

  - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

  - tenha conteúdo considerado impróprio, obsceno ou ilegal;

  - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

  - contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física, mental entre outras;

  - possua fins políticos locais ou do país (propaganda política);

  - inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

Internet

O acesso à Internet dentro da rede interna da CAPESESP é controlado e monitorado, devendo a liberação de acesso a sites ser formalmente autorizada pela diretoria responsável pelo usuário.

O acesso à Internet é liberado das 12h às 13h, diariamente, para que os colaboradores possam tratar de assuntos particulares, obedecendo sempre ao disposto nesta Política.

Os sites que possuam os conteúdos, abaixo, são bloqueados, por padrão, na CAPESESP, para todos os usuários:

- violência, ódio e racismo;
- roupas íntimas e de banho;
- nudismo;
- pornografia;
- armas;
- conteúdo adulto;
- ocultismo;
- drogas ilegais;
- conhecimentos ilegais;
- de caráter sexual;
- jogatina;
- consumo de álcool e fumo;
- chats e instant messaging;
- prática de aborto;
- corretagem online;
- jogos;
- hacking;
- encontros amorosos;
- leilões;
- redes sociais;
- malware;
- radicalizações e extremismo.

Toda informação que é acessada, transmitida ou recebida na Internet, a partir da rede interna da CAPESESP, está sujeita à auditoria. Portanto, a CAPESESP se reserva o direito de monitorar e registrar todos os acessos à Internet.

Instalação de Software

Todos os computadores em uso na CAPESESP são disponibilizados pela DSO com os softwares necessários ao trabalho do colaborador.

Qualquer software específico que se faça necessário à atividade desenvolvida pelo colaborador deve ser solicitado pelo respectivo diretor à DSO. **É expressamente vedada a instalação de qualquer software em computador da CAPESESP sem o conhecimento prévio da DSO.**

Utilização dos Discos Locais dos Computadores

É vedada a gravação de arquivos ou pastas nos discos locais (disco C:\) dos computadores da CAPESESP.

Além de não ser garantida a segurança através da política de backup, o dado gravado em disco local não obedece aos padrões de segurança adotados pela CAPESESP, estando em desacordo com o estabelecido pela LGPD.

Todos os dados relativos às atividades da CAPESESP devem ser gravados nos discos de rede e/ou nas áreas da nuvem Microsoft Office 365, disponibilizadas pela CAPESESP (One Drive e Sharepoint).

Esta Política também veda a gravação de dados de cunho particular (músicas, filmes, fotografias etc.) nos computadores da CAPESESP, seja em discos locais, de rede ou de nuvem. Caso seja identificada a presença desses tipos de arquivos nos discos de rede, os mesmos serão excluídos sem prévia comunicação.

Mesa Limpa e Tela Limpa

As informações pessoais e/ou confidenciais, independentemente do formato (físico ou digital), não devem ficar expostas sobre as mesas de trabalho e impressoras, a fim de se evitar o acesso não autorizado ou o vazamento de informação.

A tela do computador também deve ser bloqueada quando o colaborador não estiver na sua estação de trabalho, para evitar que outra pessoa tenha acesso ao conteúdo.

Ao final do expediente diário de trabalho o computador deverá ser desligado, exceto o do colaborador que possuir autorização prévia da DSO para não efetivação desse procedimento.

Comunicação Verbal

Somente os empregados devidamente autorizados podem se comunicar, em qualquer meio, em nome da CAPESESP.

Os empregados não devem tratar de assuntos internos da CAPESESP em locais públicos ou quando próximos a visitantes e/ou terceiros.

Engenharia Social

Engenharia Social é o nome dado à técnica de enganar pessoas através de mensagens ou outras formas de comunicação, com o intuito de obter informações sigilosas.

Os golpes mais comuns, hoje, na Internet, são:

- **Furto de Identidade** ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas. Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade;

- **Fraude de Antecipação de Recursos** ou *advance fee fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício;

- **Phishing** ou *phishing-scam* ou *phishing/scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social;

- **Golpes de Comércio Eletrônico** - são aqueles nos quais golpistas, com o objetivo de obter vantagens financeiras, exploram a relação de confiança existente entre as partes envolvidas em uma transação comercial;

- **Boato** ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

A CAPESESP provê ferramentas automatizadas para bloqueio de tentativas de golpes através de engenharia social, mas, caso o empregado suspeite de um possível ataque, o mesmo deverá comunicar imediatamente à DSO, através do e-mail **atendimento.dso@capesesp.com.br**.

Acesso e Trabalho Remoto

O trabalho remoto deve ser autorizado pelo gestor da área do colaborador e o acesso à VPN deve ser solicitado diretamente à DADM.

O colaborador que trabalhará em modo remoto deverá se responsabilizar pela segurança física e lógica do computador em sua residência, quanto às atualizações obrigatórias de segurança do sistema operacional e deverá possuir software antivírus devidamente atualizado.

Assim que terminada a necessidade do trabalho remoto, o gestor imediato deverá comunicar imediatamente à DADM, para que o acesso remoto seja desautorizado.

Política de Senhas

As senhas de acesso aos sistemas da CAPESESP são pessoais e devem ser mantidas em local protegido. **É vedado o compartilhamento das senhas.**

Somente os empregados da DSO possuem senhas de acesso do tipo "administrador", mediante autorização do gerente da divisão.

Recomenda-se o uso de senhas fortes, que não possuam dados como data de nascimento, endereço ou outras informações pessoais do usuário que possam ser facilmente descobertas por criminosos.

A Política de Senhas da CAPESESP estabelece algumas regras, quais sejam:

Modelo de Senha	*Nível de Segurança*
Desbloqueio da Senha	Somente pelo Administrador do Sistema
Senha Padrão	Deve ser alterada no primeiro login
Regra de Formação	caracteres especiais (@, #, $, %) e, pelo menos, um número
Tamanho Mínimo	6 (seis) caracteres
Bloqueio	Após 5 (cinco) tentativas inválidas
Prazo de Expiração	6 meses
Modelo de Armazenamento	Criptografado

Política de Backup

Os backups dos dados constantes dos servidores da CAPESESP são realizados de forma automatizada, preferencialmente fora do horário comercial, onde há pouco ou nenhum acesso de usuários.

No caso de necessidade de restauração de algum arquivo ou pasta do backup, o empregado deverá abrir um chamado técnico através do e-mail **atendimento.dso@capesesp.com.br**, informando a necessidade de recuperá-lo.

A solicitação para restauração deverá conter, discriminadamente, os nomes dos arquivos e a localização nas pastas de rede, bem como a data em que devem ser recuperados.

O detalhamento dos dados que são salvos e a frequência são documentados pela DSO na Política de Backup e aprovados pela Diretoria de Administração.

Dispositivos Pessoais

Não é permitido o uso de dispositivos pessoais (telefones celulares, tablets, videogames, notebooks etc.) conectados na rede corporativa da CAPESESP, seja através do cabeamento físico ou da rede sem fio.

O acesso à rede sem fio da CAPESESP deve ser autorizado previamente pela DADM.

Utilização de Software de Mensagens Instantâneas

A CAPESESP autoriza a utilização dos sistemas de mensageria eletrônica Microsoft Teams e Spark. Todos os computadores da CAPESESP possuem esses aplicativos e a comunicação interna deverá ser realizada através desses softwares. Quaisquer outros softwares são bloqueados e não devem ser utilizados.

É importante ressaltar que o colaborador deve sempre preservar o sigilo e a confidencialidade das informações trafegadas através de mensagens instantâneas, atendendo aos requisitos desta Política e respeitando a legislação vigente.

Videoconferência

A CAPESESP utiliza os sistemas de videoconferência Zoom e Microsoft Teams. A utilização dessas ferramentas deve ser para tratar de reuniões que tenham relação com o trabalho desenvolvido pela CAPESESP. É vedada a utilização para assuntos particulares.

É possível o uso de outros softwares de videoconferência, desde que a reunião tenha sido convocada por um usuário externo. Nesse caso, o colaborador deve solicitar antecipadamente à DSO que configure o computador com o software necessário à reunião.

Acessos aos Sistemas Corporativos

As concessões de acessos aos diversos sistemas da CAPESESP devem ser solicitadas pelo gestor imediato, por meio de abertura de chamado técnico pelo e-mail **atendimento.dso@capesesp.com.br**, informando quais os acessos do empregado.

O gestor somente poderá conceder os acessos a que ele já possua para os seus subordinados.

Os direitos de acesso aos recursos computacionais deverão sempre se limitar àqueles estritamente necessários para a execução das atividades vigentes de usuário da CAPESESP.

Todo tipo de acesso às informações corporativas e aos recursos computacionais da CAPESESP que não for explicitamente autorizado é por padrão "restrito", ou seja, proibido.

A CAPESESP reserva-se ao direito de revogar ou limitar o acesso a qualquer recurso computacional por ela concedido, temporária ou definitivamente conforme suas necessidades, visando preservar a segurança das informações e/ou garantir o desempenho dos serviços de TI diante da capacidade instalada do ambiente.

Nas alterações de cargo, transferências de setor ou de unidade, o superior imediato deverá solicitar a revogação das antigas permissões e/ou a inclusão das novas através de chamado técnico: **atendimento.dso@capesesp.com.br**.

A designação do usuário, para fins de autenticação nos Sistemas Corporativos,obedece a uma nomenclatura padronizada devendo:

- Iniciar por "us" quando o usuário estiver lotado no Nível Central ou por "re" quando for de um Escritório (Regional ou Local).

- O restante da composição do username conterá os quatro caracteres iniciais do nome completo do usuário.

Será fornecida uma senha inicial para o usuário, que deverá ser o próprio username e, no primeiro logon, será solicitada a troca da senha.

A senha definitiva deverá atender aos critérios aprovados nesta Política.

É recomendável a segregação dos ambientes para cada sistema, sendo exigida a adoção mínima de dois ambientes. A classificação dos ambientes deve seguir a nomenclatura padrão:

- **Desenvolvimento & Testes** – ambiente destinado a manter os pacotes e customizações em desenvolvimento pela equipe técnica, bem como a realização de testes de qualidade pela TI;

- **Homologação** – ambiente destinado à realização dos roteiros de testes isolados e integrados pelos usuários, simulando os retornos esperados no ambiente de produção;

- **Produção** – ambiente destinado à operação dos sistemas corporativos da CAPESESP.

Os sistemas corporativos possuem a segregação de ambiente, conforme o quadro abaixo:

Sistema	*Segregação de Ambientes*	*Regras de Concessão de Acesso*
Sistema Central	Desenvolvimento & Testes, Produção	Acesso concedido por usuário ao nível de Sistema/Módulo
Sistemas Java	Desenvolvimento & Testes, Homologação, Produção	Acesso concedido por Perfil ao nível de funcionalidade do Sistema/Módulo
Protheus	Desenvolvimento & Testes, Homologação, Produção, Treinamento	Acesso concedido por Perfil ao nível de funcionalidade do Sistema/Módulo, sendo possível aplicar regra ao nível de campo da tela
TotalPrev	Desenvolvimento & Testes, Homologação, Produção	Acesso concedido por Perfil ao nível de funcionalidade do Sistema/Módulo
RM	Desenvolvimento & Testes, Produção	Acesso concedido por Perfil ao nível de funcionalidade do Sistema/Módulo
Business Intelligence	Produção	Acesso concedido a um grupo de usuários
Hotsite Conselhos	Desenvolvimento & Testes, Produção	Acesso concedido por Perfil ao nível de funcionalidade de cada área restrita Autenticação via Login e Assinatura Eletrônica
Portal Internet e Intranet	Desenvolvimento & Testes, Produção	Acesso concedido por Perfil ao nível de funcionalidade Autenticação via Login e Assinatura Eletrônica

SISTEMA CENTRAL

O acesso ao Sistema Central é realizado em dois passos: 1º) autenticação no servidor Linux; e 2º) acesso ao menu principal da aplicação, filtrando os acessos concedidos aos módulos.

O Sistema Central possui ambientes segregados destinados a Desenvolvimento & Testes e Produção.

SISTEMAS JAVA

O acesso aos Sistemas Java, que compreendem o Sistema de Contabilidade, Controle de Estoque e Cadastro de Fornecedores, atende à regra padrão dos Sistemas Corporativos, possuindo o controle de perfil de acesso ao nível de funcionalidades dos módulos do sistema.

Os Sistemas Java possuem ambientes segregados destinados a Desenvolvimento, Homologação e Produção.

SISTEMA PROTHEUS

O acesso ao Sistema Protheus é realizado através do "*SmartClient*" (aplicação da TOTVS que é a responsável pelo acesso ao sistema Protheus) instalado na estação de trabalho e de acordo com o perfil de acesso do usuário são disponibilizados os módulos e funcionalidades do sistema.

O Dono da Informação do Sistema Protheus será responsável por manter a Política de Perfil de Acesso e Matriz de Responsabilidade atualizada.

O Sistema Protheus possui ambientes segregados destinados a Desenvolvimento & Testes, Treinamento, Homologação e Produção.

A regra de criação de usuários para o ambiente de produção do Sistema Protheus atende à regra padrão dos Sistemas Corporativos, havendo uma regra diferenciada para os demais ambientes.

TOTALPREV

O acesso ao Sistema de Previdência TotalPrev é realizado através de login do próprio sistema e de acordo com o perfil de acesso do usuário concedido ao nível de funcionalidades dos módulos.

O Sistema TotalPrev possui ambientes segregados destinados a Desenvolvimento & Testes e Produção.

BUSINESS INTELLIGENCE (BI)

O sistema de Business Intelligence utiliza o software QlikSense e é acessado através do link **bi.capesesp.com.br**.

O sistema tem login próprio e há contas de acesso para cada diretor, AEI, DPAS, DADM, DAFI e DRA.

Cabe à AEI a segregação dos universos, oferecendo visões correspondentes ao que cada login de acesso deverá possuir.

SISTEMA RM

O Sistema RM é o aplicativo de Recursos Humanos da empresa TOTVS e o acesso administrativo é de uso exclusivo da Divisão de Recursos Humanos da CAPESESP.

O sistema contempla os módulos de Folha de Pagamento, Portal RH, Automação de Ponto e Gestão de Pessoas.

O sistema é executado na modalidade ASP (Application Service Provider), onde os programas e os bancos de dados estão hospedados no ambiente da empresa fornecedora (TOTVS).

O acesso dos demais colaboradores ao Portal de RH do sistema RM é concedido pela DRH, no momento da admissão do empregado, com o nível de permissão diferenciado em caso de gerentes ou diretores.

A autenticação do usuário no portal de RH se dá pela matrícula funcional. A senha inicial é o CPF do empregado e deve ser trocada no primeiro acesso.

O Sistema RM possui ambientes segregados destinados a Desenvolvimento & Testes e Produção.

HOTSITE DOS CONSELHOS

O acesso ao hotsite dos Conselhos Deliberativo e Fiscal (http://www.capesesp.com.br/conselho) é restrito aos conselheiros efetivos da CAPESESP e aos colaboradores indicados pela Presidência.

O acesso a esse hotsite deve ser solicitado ao Diretor-Presidente pela Secretaria Geral da Presidência.
A autenticação no hotsite deve ser feita duplamente, fornecendo o login de acesso primário ao site CAPESESP (login e senha) e depois através da validação da assinatura eletrônica para acesso à área restrita do site.

PORTAL DE INTERNET

O Portal de Internet da CAPESESP (http://www.capesesp.com.br) possui diversos serviços que podem ser acessados por seus associados e por seus colaboradores, inclusive, representantes da rede de atendimento do CAPESAÚDE (credenciados).

Os acessos são automaticamente liberados quando o associado ou credenciado é cadastrado no Sistema Central.

Uma senha inicial de acesso é automaticamente gerada pelo sistema e informada ao associado ou credenciado. Esses usuários devem alterar a senha no primeiro acesso ao site da CAPESESP.

Para acesso ao módulo de Concessão de Empréstimos da CAPESESP, como segurança adicional, é solicitado ao associado criação da assinatura eletrônica.

PORTAIS DE INTRANET

Os serviços do portal de Intranet (**http://www.capesesp.com.br/servicos**) são acessados através de autenticação pela matrícula funcional do colaborador, sendo exigida a assinatura eletrônica para acesso ao módulo de Concessão de Empréstimos da CAPESESP.

Acesso a Banco de Dados

É expressamente vedado o acesso direto aos bancos de dados dos sistemas, seja em ambiente de produção, desenvolvimento ou testes. O acesso de usuários às informações mantidas em banco de dados deve ser feito somente por meio de sistemas de informação e não de forma direta.

Somente os colaboradores da área de desenvolvimento de sistemas (DSI) deverão possuir acesso direto aos bancos de dados, sendo esclarecido que **não é permitida a extração de quaisquer tipos de dados pessoais externos aos bancos de dados**, seja em planilhas ou arquivos texto.

Horários de Acesso aos Sistemas

É expressamente vedado o acesso a qualquer sistema da CAPESESP fora do horário de trabalho estipulado pelo contrato de trabalho celebrado entre o colaborador e a CAPESESP, com exceção a casos autorizados previamente pela DADM.

Desligamento de Colaboradores

Após conclusão do processo de desligamento do colaborador, a DRH deverá imediatamente enviar um comunicado para a DLG, visando o bloqueio aos acessos físicos, e para a DSO o bloqueio de acessos lógicos.

A partir do momento do recebimento do comunicado, a DSO deverá efetuar o bloqueio de todos os acessos aos sistemas e ao e-mail corporativo.

A caixa de e-mail do ex-empregado poderá ser conectada à caixa de e-mail do gestorda área, caso seja solicitado.

Regra geral, o equipamento do ex-colaborador será formatado pela DSO e preparado para ser designado ao substituto deste usuário, ou para compor o rol de equipamentos de backup.

Acesso às Pastas Departamentais e Regionais

A CAPESESP disponibiliza alguns discos de rede para que os usuários possam salvar os arquivos de trabalho. Esses discos de rede estão cadastrados nas rotinas de backup da DSO. Quaisquer arquivos ou pastas gravadas em discos locais dos computadores não serão salvos em backup.

A estrutura de discos de rede varia de acordo com o local de trabalho, conforme demonstrado abaixo:

NÍVEL CENTRAL

Os usuários do Nível Central, ao se conectarem na rede local, terão automaticamente mapeados os seguintes discos de rede em sua estação de trabalho:

Disco	Descrição	Nível de Segregação	Permissão de Acesso	A que se destina
P:\	Disco Público	Por Diretoria PRE, DADM, DPAS, DAFI	Leitura Pública Gravação por Diretoria	Compartilhamento de documentos e projetos da CAPESESP
Q:\	Disco Compartilhado	Por Diretoria e Divisão	Leitura da Diretoria Gravação por Divisão	Compartilhamento de assuntos internos da Diretoria
R:\	Gravação de CD e DVD	Por Divisão	Leitura e Gravação por Divisão	Envio de conteúdo para gravação de mídia
S:\	Disco de Softwares	Não se aplica	Leitura Pública Gravação pela DSO	Acesso a software corporativo
T:\	Disco de Trabalho	Por Divisão Por Coordenador Por Diretor	Leitura/Gravação Divisão Leitura/Gravação Gerente Leitura/Gravação Diretor	Compartilhamento de assuntos internos da Divisão

Disco Público P: - onde estão localizados arquivos e pastas públicos da CAPESESP, tais como documentos do CDP (Controle de Documentos Padronizados), projetos diversos e áreas públicas de cada diretoria.

Nesse disco há uma pasta referente a cada diretoria da CAPESESP (PRE, DPAS, DADM e DAFI). Nessas pastas, o acesso à leitura é público e à gravação é permitido somente aos componentes da respectiva diretoria.

Disco Compartilhado Q: - rede compartilhada da diretoria. Cada diretoria da CAPESESP possui um disco Q:\ diferente, onde somente os subordinados possuem acesso.

Dentro desse disco há uma pasta com o nome de cada divisão de trabalho da CAPESESP. Nessa pasta, somente os integrantes da divisão e os diretores dessa diretoria possuem acesso.

Disco de gravação de mídia R: - destinado à gravação de CD e DVD. Quando um usuário da CAPESESP necessitar gravar uma mídia, deve colocar os arquivos na pasta correspondente à sua divisão e solicitar à DSO a gravação através de chamado técnico. Os usuários somente possuem acesso à pasta referente à sua divisão.

O conteúdo dessas pastas é automaticamente apagado a cada sábado.

Disco de Softwares S: - contém alguns softwares utilizados na configuração de aplicativos utilizados na CAPESESP.

Disco de área de trabalho T: - contém a área de trabalho da divisão. Cada divisão da CAPESESP possui um disco T:\ diferente, com permissões de gravação e leitura somente aos integrantes da sua divisão.

Dentro desse disco de rede há uma pasta chamada coordenador ou diretor, onde o acesso é somente permitido ao gerente da divisão ou diretor, no caso de uma diretoria.

ESCRITÓRIOS REGIONAIS

As estações de trabalho dos Escritórios Regionais estão conectadas através de uma rede ponto a ponto, onde não há servidor central.

Para fins de compartilhamento de arquivos de trabalho no Escritório Regional, é eleita uma estação de trabalho como servidor de arquivos, sendo configurada e compartilhada uma pasta do disco local intitulada de "C:\TRAB--GER". As outras estações de trabalho mapeiam esse compartilhamento de rede através do disco T:\.

É recomendado aos colaboradores dos Escritórios Regionais que salvem os seus arquivos e pastas de trabalho somente no disco de rede T:\. Todo e qualquer arquivo armazenado fora deste disco não possuirá backup.

Visando à segurança dos arquivos de trabalho do Escritório Regional, é eleita uma segunda estação de trabalho como servidor de backup, sendo configurada uma pasta de nome "C:\TRAB-BACKUP" e um script batch que efetua uma cópia do conteúdo da pasta de trabalho T:\ para a pasta "C:\TRAB-BACKUP". Essa rotina é manual e deve ser acionada diariamente por um empregado indicado pelo gerente regional.

MICROSOFT OFFICE 365

Adicionalmente, são oferecidos recursos na nuvem Microsoft Office 365 para que os usuários possam salvar os seus arquivos.

Sharepoint – A DSO cria sites virtuais no aplicativo Sharepoint para que as áreas de trabalho possam salvar os arquivos que são departamentais. Essa estrutura é compartilhada entre todos os membros da divisão ou Escritório Regional e confere segurança e o versionamento dos arquivos.

OneDrive – Recurso oferecido a todos os usuários para salvar arquivos individuais na nuvem Office 365. Os arquivos salvos no OneDrive têm acesso exclusivo ao próprio usuário, mas há a possibilidade de compartilhá-los com outros usuários.

Deve ser tomado o cuidado de não compartilhar dados pessoais com usuários externos, de forma a atender à Lei Geral de Proteção de Dados Pessoais.

Revisão de Acessos

As revisões de acesso devem ser realizadas com periodicidade anual, objetivando adequar os acessos concedidos aos requisitos de segurança estabelecidos nesta Política.

Escopo da revisão	Periodicidade da Revisão	Executor da Revisão
Banco de Dados	Anual ou Eventual	DSO
Sistemas de Informação	Anual ou Eventual	DSI e DSO
Recursos de Rede	Anual ou Eventual	DSO
Testes vulnerabilidade da infraestrutura de segurança	Anual	Consultoria especializada contratada

Os gestores que são Donos da Informação poderão solicitar a qualquer tempo a revisão de acesso dos sistemas ou recursos de rede sob a sua responsabilidade.

A DSO é responsável por coordenar as seguintes atividades de revisão de acessos:

- Comparação da lista de acessos concedidos a empregados com a lista atualizada do quadro de pessoal da CAPESESP;

- Comparação da lista de acessos concedidos a prestadores de serviço, inclusive “temporários”, considerando as informações fornecida pela DRH e DLG;

- Homologação formal pelos Donos da Informação, encaminhando lista atualizada dos Perfis de Acesso e Matriz de Responsabilidade dos sistemas de informações sob a sua responsabilidade;

Realização periódica do teste de vulnerabilidade da infraestrutura de segurança, visando detectar necessidades de aprimoramento das regras de segurança relativas à rede de dados e internet da CAPESESP. Deverão ser propostos projetos de implementação de melhorias de segurança objetivando a correção das vulnerabilidades detectadas.

Utilização de Mídias Removíveis

A porta USB do computador é um importante ponto de vulnerabilidade de segurança, especificamente com o uso de pendrives ou discos externos, pois pode ser usada para fuga de informação e o seu uso não está em conformidade com a LGPD.

Por esse motivo, o uso de mídias removíveis e portas USB dos computadores é bloqueado por padrão, para todos os computadores da CAPESESP. Caso seja imperioso para a execução da atividade de trabalho do colaborador, a liberação desse acesso deve ser solicitada pelo gestor imediato à DADM.

As portas USB dos computadores são liberadas somente para o uso de dispositivos de entrada de dados, como teclados, mouses e headsets, bem como para os assinadores digitais.

Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais - LGPD prevê que todos os colaboradores que manipulam dados pessoais ou sensíveis obedeçam ao que está descrito na lei e na Política de Privacidade de Dados da CAPESESP.

Entende-se por bases de dados com dados pessoais quaisquer documentos físicos (requerimentos, certidões, declarações, currículos etc.) ou documentos digitais (planilhas Excel, documentos Word, bancos de dados Access, arquivos de texto etc) que contenham algum dado pessoal.

No caso do documento digital, o colaborador que criou o documento é o responsável pela confidencialidade, integridade e disponibilidade.

Algumas orientações devem ser atendidas para a proteção dos dados pessoais, a saber:

- Estar disponíveis somente no tempo necessário para o seu tratamento. No momento em que os dados já não forem mais necessários, devem ser descartados.

- Devem ser mantidos em locais protegidos, garantindo que somente os usuários autorizados tenham acesso a esses dados.

- É vedada a realização de cópias externas ou compartilhamento externo de bases de dados que contenham dados pessoais.

A **Política de Privacidade de Dados da CAPESESP** está disponível para consulta no site (www.capesesp.com.br).

Divulgação e Treinamento

A DRH e a DSO deverão definir um Plano de Divulgação e Treinamento para que todos os colaboradores possam tomar ciência da Política de Segurança da Informação.

Todos os colaboradores deverão assinar o Termo de Compromisso e Ciência.

Tratamento de Violações

Os indícios de infrações das normas de segurança previstos nesta Política deverão ser notificados à Comissão de Ética da CAPESESP (comissão.etica@capesesp.com.br) que examinará o caso, nos termos do Código de Ética e de Padrões de Conduta Profissional da CAPESESP.

Vigência, Validade e Atualizações

A presente Política passa a vigorar a partir da data de sua aprovação pela DiretoriaExecutiva da CAPESESP, sendo válida por tempo indeterminado.

Com o objetivo de manter esta Política sempre atualizada, deverão ser realizadas anualmente, ou quando houver incidentes, revisões em seu texto, com as modificações que se julgarem necessárias.

Referências

ABNT NBR ISO/IEC 27001:2006 Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.

CAPESESP - Código de Ética e de Padrões de Conduta Profissional.

CERT.BR – Cartilha de Segurança para Internet.

ISO/IEC 27000:2018 Information technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary

Lei nº 9.609/98 – Lei do Software - Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

Lei nº 12.527/11 – Lei de Acesso à Informação - Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Lei nº 12.737/12 – Lei Carolina Dieckmann - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

Lei nº 12.965/14 – Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Lei nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD).

TCU – Boas Práticas em Segurança da Informação (2012).

Controle de Versões			
Versão	**Data**	**Autor**	**Notas da Revisão**
1.0	06/01/2012	Elina Cabral	Primeira versão
2.0	08/03/2021	Artur B. Torres	Atualização da PSI

Glossário e Definições

Acesso - Credencial que possibilita aos usuários fazer uso de serviços, dados ou outros ativos de TI.

AEI – Assessoria de Estratégias e Informações Institucionais.

Aplicativo - Programa ou software que provê as funções requeridas por um serviço de TI, em geral desenvolvido para executar um tipo particular de trabalho e facilitar a utilização de rede interna de microcomputadores.

Assinatura eletrônica - Código secreto individual que é solicitado no site da CAPESESP para acesso ao módulo de solicitação de empréstimos. A assinatura eletrônica é criada pelo próprio associado e funciona como uma segunda chave de acesso, fornecendo maior segurança ao serviço de solicitação de empréstimos.

Ativo de Informação - Qualquer tipo de informação que possui significado ou valor para a entidade, que não pode ser facilmente substituída sem custo, ou emprego de habilidade, tempo, recursos, ou uma combinação desses itens. Abrange a informação em formato digital ou não digital, que é criada, processada, armazenada ou apagada durante a execução de atividades na CAPESESP.

Backup - Cópia de segurança, gravada em mídia eletrônica, para uso em caso de perda dos originais, ou para resgatar uma posição histórica.

Bens de Informação - São os componentes da Tecnologia da Informação - TI: sistemas, aplicativos desenvolvidos e adquiridos, softwares básicos e de apoio, dados, hardware, instalações físicas e equipamentos de infraestrutura.

Bloqueio/Proteção de Tela - Comando que indica o bloqueio de uma estação de trabalho. Quando o usuário bloqueia a estação, ao deixá-la por um determinado tempo, seus acessos permanecem indisponíveis para que qualquer outra pessoa os utilize.

Colaborador - empregados da CAPESESP que integram o seu quadro de pessoal, os estagiários e os menores aprendizes a ela vinculados e, adicionalmente, prestadores de serviços e seus empregados que exerçam suas atividades dentro ou fora das dependências da CAPESESP.

Confidencialidade - Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Criptografia - Técnica que consiste na aplicação de algoritmos matemáticos para alterar e embaralhar as informações, de forma que somente quem tenha o mesmo algoritmo que cifrou a informação possa decifrá-la para leitura e uso.

DADM – Diretoria de Administração.

DAFI – Diretoria de Administração Financeira.

Dado Pessoal - Informação relacionada a pessoa natural que possa identificá-lo ou torná-lo identificável.

Dado Pessoal Sensível - Relacionado à pessoa física, identificada ou identificável, que trate sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político ou que se refere à saúde ou à vida sexual e dado genético ou biométrico.

Dado Anonimizado - Dado relativo ao titular que não possa identificá-lo, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Depositário dos dados (custodiante) - Responsável pelo processamento, armazenamento e custódia das informações.

Disponibilidade - Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

DLG – Divisão de Logística.

DRA- Divisão de Rede de Atendimento.

DRH – Divisão de Recursos Humanos.

DPAS – Diretoria de Previdência e Assistência.

DSI – Divisão de Sistemas de Informação.

DSO- Divisão de Suporte e Operação.

Estação de Trabalho - Microcomputador conectado ao servidor de rede. O equipamento acessa o software no servidor e realiza o processamento na própria estação, podendo o armazenamento dos dados ser realizado em ambos os equipamentos.

Incidente de Segurança da Informação - Um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Informação - Dados estruturados, dotados de relevância e propósito para a instituição.

Integridade - Propriedade de salvaguarda da exatidão e completeza de ativos.

Inventário - Documentação que visa guardar informações relativas a ativos físicos (equipamentos e mobiliário) e softwares (licenças de uso).

LGPD - Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.

Login – É o ato de se identificar ao sistema. Essa identificação permite o acesso de um usuário a um determinado serviço e concede a ele todas as autorizações que estão habilitadas para essa conta.

Logout/Exit/Desligar - Comando que indica a saída do usuário da rede ou sistema. Quando o usuário deixa de executar o logout em sua máquina, ao terminar uma atividade na rede, seus acessos permanecem disponíveis para que qualquer outra pessoa a utilize.

Política de Segurança da Informação - Um conjunto de medidas necessárias à preservação e segurança dos bens e ativos de informação da empresa.

PRE – Presidência.

Proprietários das informações - São os empregados responsáveis pela informação na CAPESESP. Normalmente estas funções são atribuídas ao gerente de cada área, conforme estrutura organizacional.

Recursos Computacionais - Todo equipamento ou dispositivo (hardware), aplicativo ou sistema (software), ou serviço de tecnologia da informação envolvido no processamento ou transmissão da informação. Alguns exemplos: telefone, celular, computador, notebook, servidor, rede de dados corporativa, sistemas de informação, intranet, internet, web conferência.

Rede Interna - Considera-se Rede Interna para efeito normativo, o ambiente interno da CAPESESP, configurando-se este por meio da conexão e comunicação de equipamentos de informática (microcomputadores, terminais, impressoras etc), de modo a permitir a seus usuários compartilharem recursos e informações.

Restore - O mesmo que restaurar ou retornar um backup de arquivo, banco de dados, aplicativos/sistemas, pasta, diretório de trabalho ou e-mail e que se exista dentro da rotina de cópia de segurança.

Servidor - Computador conectado à rede, que fornece funções de software usadas por outros computadores.

Senha (*password*) - Código secreto individual, que permite acesso aos bens ou ativos de informação que possuem controle de acesso.

Sistemas Aplicativos/Corporativos - Sistemas de processamento das informações corporativas e departamentais da CAPESESP.

Termo de Compromisso e Ciência - Documento que tem por objetivo formalizar e esclarecer aos usuários sobre a importância das informações pessoais, departamentais e corporativas, tornando-os responsáveis pelas ocorrências que envolverem o uso dos recursos computacionais sem a aplicação de metodologias e segurança.

Usuário - Pessoa que opera, interage ou utiliza diretamente um produto ou serviço de tecnologia da informação no dia a dia. Ou seja: todo dirigente, empregado, terceiro, estagiário, consultor e visitante, que tenha acesso aos bens ou ativos de informação da CAPESESP.

Aprovada pela Diretoria-Executiva em 09/04/2021 (Ata DE Nº 05).

Termo de Responsabilidade

Este Termo lista as responsabilidades dos usuários de recursos de tecnologia da informação da CAPESESP, estando de acordo com os princípios da Confidencialidade, Disponibilidade e Integridade que fundamentam a Política de Segurança da Informação da entidade. Seu objetivo visa ao uso ético e responsável dos recursos pelos empregados e prestadores de serviço.

Aceito cumprir e declaro ter pleno conhecimento da Política, Normas e Procedimentos de Segurança da Informação da CAPESESP, que trata dos aspectos da informação processada a partir dos recursos de TI da empresa: mensagens eletrônicas, internet, bancos de dados, mídias de áudio e de vídeo, arquivos eletrônicos e relatórios impressos.

Assumo a responsabilidade, civil e/ou criminal, pela utilização indevida do direito de propriedade intelectual das informações processadas nos recursos informatizados da CAPESESP.

Tenho ciência de que a assinatura deste Termo constitui observar as seguintes responsabilidades:

1. Utilizar qualquer recurso de TI da empresa somente após obter a autorização, nos termos dessa Política;

2. Respeitar a integridade da autorização de acesso concedida, com o compromisso de não revelar ou compartilhar minha senha de acesso aos sistemas corporativos e demais Serviços de TI, além de adotar as recomendações de utilização de senha para documentos confidenciais, conforme recomendações da Política de Segurança da Informação da CAPESESP;

3. Não excluir, copiar ou alterar informações transmitidas, produzidas ou armazenadas nos recursos computacionais para fins adversos às rotinas de trabalho, uma vez que todo material desenvolvido nas instalações da CAPESESP é considerado propriedade intelectual da entidade;

4. Não vender ou negociar o conteúdo, material, software, produto, serviço ou informação obtida nos recursos de TI da empresa ou utilizá-los com propósitos imorais ou ilícitos;

5. Não utilizar as informações com fins de criação, transmissão, procura, instalação, impressão, armazenamento ou envio de conteúdo difamatório, grosseiro, ofensivo, prejudicial ou ameaçador, relacionado à violência, profanação, ódio, racismo, assédio, discriminação, drogas, jogos de azar, pedofilia ou pornografia, ou ainda, material calunioso, abusivo ou que invada a privacidade alheia;

6. Não instalar, enviar ou armazenar nos servidores de rede material não protegido pelas leis de direitos autorais e de propriedade, jogos eletrônicos, piadas, cartões, cartas de correntes, vídeos, fotos ou outro conteúdo que não esteja relacionado ao trabalho desenvolvido ou que configure crime virtual;

7. Tratar as informações institucionais de acordo com as normas de classificação abaixo:

7.1.1. Informações confidenciais e ou de acesso restrito da CAPESESP não podem ser transportadas em qualquer mídia sem as devidas autorizações e proteções.

7.1.2. Assuntos confidenciais não devem ser revelados fora dos âmbitos previstos nos regimentos internos de cada colegiado e de acordo com as disposições do Código de Ética e de Conduta Profissional da CAPESESP.

8. Documentos impressos e arquivos com informações confidenciais devem ser adequadamente armazenados e protegidos e o seu descarte deve respeitar a temporalidade e observar as recomendações da Política de Segurança da Informação da CAPESESP;

9. Armazenar os dados corporativos nas pastas de rede e servidores apropriados, não mantendo dados da empresa na estação local;

10. Usar o computador, sistema ou a rede de forma adequada e segura, para não interromper a operação normal de outros recursos computacionais, sempre respeitando o perfil de acesso concedido pela TI e as finalidades autorizadas;

11. Solicitar apoio da DSO, com abertura de chamado para configuração de recursos computacionais, inclusive para liberação dos equipamentos a VISITANTES, dando ciência ao VISITANTE das regras e restrições impostas por esta Política;

12. Não violar os direitos autorais, patentes e licenças de uso de software;

13. Não interceptar ou realizar tentativas de interrupção dos serviços de outros usuários, serviços de transmissão de dados, danos de vírus, gargalos da rede ou apropriar-me dos recursos computacionais da entidade;

14. Não utilizar o correio eletrônico para formar palavras ou expressões que gerem duplo sentido, não condizentes com o ambiente corporativo ou que possam causar danos de imagem à CAPESESP;

15. Não distribuir mensagens não solicitadas (SPAM, correntes) que possam causar excesso de tráfego e prejudicar a produtividade das equipes;

16. Não tentar invadir ou burlar sistemas de segurança, nem adivinhar identificação ou senhas de terceiros, nem interferir em sistemas de gravação;

17. Não utilizar listas de ramais ou cadernos de endereços eletrônicos da empresa para a distribuição de mensagens fora do interesse funcional;

18. Desligar a estação de trabalho ao encerrar as atividades ou utilizar a opção "*logoff*", caso a estação precise permanecer ligada;

19. Ativar o recurso de bloqueio de acesso à estação de trabalho quando afastar-se temporariamente do posto de trabalho; e

20. Zelar pela conservação dos recursos computacionais e por sua correta utilização, não retirar ou violar etiquetas que selam as unidades de CD e DVD, Portas USB, CPU.

Declaro ter ciência de que:

1. Alterações da Política, Normas e Procedimentos de Segurança poderão ser divulgadas nos canais de informação, escrita ou eletrônica, sendo incorporadas quando do meu novo acesso a estes canais; e.

2. A CAPESESP poderá monitorar e auditar o meu acesso aos Recursos Computacionais sem comunicação prévia, tendo minha concordância com este procedimento.

Reconheço a obrigação de:

1. Comunicar à Comissão de Ética (comissão.etica@capesesp.com.br) qualquer suspeita ou evidência de violação de segurança, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros;

2. Providenciar a imediata troca de senha ao suspeitar qualquer tipo de violação dos acessos a mim autorizados; e de

3. Arcar com as consequências de danos provocados pelo uso indevido dos meus acessos.

Por fim, tenho ciência de que o descumprimento das Diretrizes, Normas e Procedimentos da Política de Segurança da Informação e das obrigações dispostas neste Termo de Responsabilidade será considerado transgressão, sendo responsável pelos atos por mim praticados e sujeito às sanções previstas no Código de Ética e Conduta Profissional da CAPESESP em seu **capítulo V – Da Responsabilidade pelos atos praticados.**

Termo de Compromisso e Ciência

CAPESESP

Caixa de Previdência e Assistência dos Servidores da Fundação Nacional de Saúde

TERMO DE COMPROMISSO E CIÊNCIA
COM A POLÍTICA DE SEGURANÇA DE INFORMAÇÃO DA CAPESESP

Declaro que tomei conhecimento inequívoco da Política de Segurança de Informação da CAPESESP e do Termo de Responsabilidade, disponibilizados no Portal da Entidade, e estou ciente e de acordo com todas as regras e obrigações neles contidas, assumindo o compromisso de observá-las e bem aplicá-las na execução de minhas atividades profissionais, sob pena de sujeição às sanções nele estabelecidas.

Fica determinado que quaisquer dúvidas com relação ao presente TERMO serão esclarecidas junto à Divisão de Recursos Humanos.