NORMA DE SEGURANÇA DE INFORMAÇÕES

I-OBJETIVOS

A Norma Corporativa de Segurança de Informações da **OCB / SESCOOP** tem como objetivos:

1. Definir o tratamento a ser dado às informações no que diz respeito ao seu manuseio, propriedade e responsabilidade de uso.
2. Estabelecer os princípios básicos para a correta utilização dos recursos computacionais da Organização, a fim de evitar a perda de recursos ou informações por acidentes ou não.
3. Orientar os procedimentos de implementação a fim de garantir a integridade, disponibilidade e confidencialidade das informações.

II-AMPLITUDE

Esta norma abrange todos os ambientes físicos e lógicos designados para o processamento ou transmissão de informações, isto é, todos os equipamentos e programas de computador, locais ou remotos, bem como toda e qualquer informação processada, armazenada ou transmitida por eles.

III-CONSIDERAÇÕES GERAIS

1. Toda informação é de propriedade da **OCB / SESCOOP,** e por assim ser é um bem que tem valor e deve ser protegido, cuidado e gerenciado adequadamente.
   a. Todo arquivo armazenando nos computadores da **OCB / SESCOOP** é de propriedade dos mesmos, dessa forma, as informações contidas nos arquivos podem ser auditadas, pela Gerência de TI, e seu acesso pertence à instituição. Nesse âmbito entende-se que a propriedade de documentos, arquivos eletrônicos e e-mails são da **OCB / SESCOOP** e não do funcionário que faz uso da informação ou recurso.

SAUS - Setor de Autarquias Sul, Quadra 04, Bloco I
CEP: 70070-936 - Brasília/DF
Telefone: (0xx61) 325-5500 Fax: (0xx61) 325-8383
email: ocb@ocb.org.br

2. Todos os funcionários, contratados, incluindo prestadores de serviços, estagiários e temporários a serviço da **OCB / SESCOOP** são responsáveis pela segurança, zelo e bom uso das informações às quais têm acesso. O conhecimento das informações deverá ser utilizado apenas para o exercício profissional.
3. Os Estagiários utilizarão correio eletrônico específico e padronizado pela Gerência de TI.
4. Terceiros, tais como, palestrantes e convidados, poderão utilizar os recursos de TI, com acesso restrito, mediante solicitação do Gerente da área interessada ao Gerente de TI/Superintendente Administrativo, que analisará a pertinência e o nível de segurança da liberação.
5. As informações e os recursos de informática serão disponibilizados única e exclusivamente àqueles que necessitem para o exercício de suas funções e após terem conhecido o presente documento.
6. Cada usuário acessará o ambiente computacional através de sua identificação e senha as quais são pessoais e intransferíveis. Portanto, o usuário deve manter em absoluto sigilo a sua senha de forma que somente ele possa reproduzi-la.
7. Todas as instalações e equipamentos devem ser protegidos, pela Gerência de TI, contra acessos não autorizados.
8. Toda informação deve ser protegida para que não seja alterada, acessada ou destruída indevidamente por pessoas não autorizadas.
9. Toda informação de propriedade da **OCB / SESCOOP** deve ser armazenada no servidor e possuir cópia de segurança guardada em local protegido, compatível com o grau de segurança necessário, recomendado pela Gerência de TI.
10. Os ambientes de processamento e transmissão, centralizados e distribuídos, devem ter planos de contingência definidos, revistos e testados periodicamente.
11. Todos os dispositivos utilizados para a proteção, manutenção da integridade, disponibilidade e confidencialidade das informações devem ser considerados de absoluto sigilo, sendo, portanto, proibida a sua divulgação a pessoas não autorizadas ou a terceiros.
12. A custódia das informações processadas em equipamentos centralizados, e por eles distribuídos, é de responsabilidade da Gerência de Tecnologia da Informação bem como a custódia das informações processadas em equipamentos locais (microcomputadores) é de responsabilidade de cada Diretoria/Superintendência/Gerência que os utiliza.
13. Todo e qualquer programa de computador (software ou aplicativo) utilizado deve ser de propriedade da **OCB / SESCOOP**, devendo atender aos padrões de segurança e homologação, bem como à compatibilidade e conectividade com a arquitetura existente, não sendo permitida a instalação de qualquer componente que não tenha sido adquirido pelas mesmas.
14. Todos os contratos de terceiros devem ser homologados técnica e comercialmente prevendo o cumprimento dos padrões de segurança da **OCB / SESCOOP.**

15. Todos os funcionários e contratados, incluindo prestadores de serviços, estagiários e temporários, têm a responsabilidade de contribuir para a melhoria dos níveis de segurança de informações. Portanto, qualquer ponto de vulnerabilidade ou de melhoria deve ser comunicado imediatamente.
16. Todos os funcionários da **OCB / SESCOOP** são responsáveis por comunicar de imediato a seu superior hierárquico quaisquer irregularidades no cumprimento desta norma.

IV-PROCEDIMENTOS

1. ACESSOS, CHAVE DE ACESSO E SENHAS.

O usuário não receberá qualquer chave de acesso ou senha para acessar os sistemas da **OCB / SESCOOP** até que tenha conhecido o Termo de Responsabilidade.

A Chave de Acesso e Senha é pessoal e intransferível, sendo imprescindível que durante o primeiro acesso o sistema esteja habilitado a solicitar a troca da senha. Caso a troca da senha não seja efetivada ou realizada os próximos acessos deverão ser bloqueados e o usuário comunicado e orientado a entrar em contato com a Gerência de TI da **OCB / SESCOOP** para obter uma nova senha.

Todos os equipamentos deverão ser programados com proteção de tela mediante senha, com intervalos não superiores a 15 minutos de repouso para início do bloqueio e proteção da informação.

Os acessos aos recursos computacionais e os níveis de acesso deverão ser devidamente autorizados pela gerência imediata, através de formulário eletrônico, disponibilizado pela Gerência de TI.

Os acessos externos na rede da **OCB/SESCOOP** serão formalmente solicitados e justificados à Gerência de TI, que submeterá a apreciação e autorização do Superintendente Administrativo.

O funcionário, prestador de serviço, colaborador ou estagiário quando desligado do Sistema **OCB/SESCOOP** terá seu acesso bloqueado imediatamente a ocorrência do desligamento, cabendo ao gerente da área e a assessoria de gestão de pessoas prontamente informar à Gerência de TI para as providências cabíveis.

Os gerentes são diretamente responsáveis pela liberação de acesso à rede **OCB/SESCOOP.**

2. RESPONSABILIDADES PESSOAIS

Os sistemas de informação da **OCB / SESCOOP** contêm informações proprietárias e confidenciais. Portanto, todos os usuários são responsáveis por assegurar que os dados, informações e recursos de computação serão utilizados única, exclusiva e diretamente para suporte às práticas e negócios da **OCB / SESCOOP** a qual proverá recursos compartilhados sendo que os acessos serão de responsabilidade individual de cada usuário.

3. USO APROPRIADO DE RECURSOS

Todos os recursos computacionais da **OCB / SESCOOP** são intencionados para propósitos de negócio. O uso de qualquer recurso, ou parte dele, para outras finalidades é proibido estritamente. Também são proibidas atividades, componentes, ou aplicações que não são especificadas diretamente como parte dos padrões de Recursos Computacionais.

São, portanto, vedadas a todos os usuários:

1. Copiar, ceder ou facilitar acesso, para pessoal não autorizado, a arquivo ou informação de propriedade da **OCB/SESCOOP,** de uso profissional, inclusive aquelas que sabe não ser de caráter sigiloso.
2. Utilizar versões não legais e/ou não registradas de programas de computador bem como a cópia de qualquer aplicação ou dados para uso externo ou alheio aos interesses da **OCB / SESCOOP;**
3. Adicionar qualquer tipo de periféricos de comunicação às estações de trabalho para conexão externa ou interna ou delas se valer para sondar, vasculhar ou estabelecer conexão aos recursos de rede da **OCB / SESCOOP** sem que para tal estejam habilitados ou autorizados.
4. Tentar obter direitos ou acesso diferente daqueles especificados e apropriados ao exercício de suas funções ou executar ou desenvolver programas que possam hostilizar outros usuários ou prejudicar o bom funcionamento dos recursos computacionais.
5. Utilizar o sistema de correio eletrônico (E-mail) para enviar mensagens fraudulentas, hostis, obscenas, eróticas, ameaças ou outras mensagens ilícitas, incluindo a criação, envio ou compartilhamento de mensagens em atenção a sorteios ou sistemas de ajuda mútua (cartas de cadeia, pirâmide etc.).
6. Acessar "sites" da Internet que ferem os interesses da **OCB / SESCOOP** ou que tenham estrutura e origem duvidosa.
7. Tornar disponível na Internet qualquer informação da **OCB / SESCOOP** sem consentimento expresso das Gerências.
8. Acessar, sem autorização prévia, sites para acesso a correio eletrônico particular e chat, que não seja o corporativo da **OCB / SESCOOP.**
9. Acessar sites de conteúdo erótico, bate-papo, e demais websites da Internet que não tenha ligação direta ou indireta com o exercício das atividades profissionais.

4. AUDITORIA

A **OCB / SESCOOP** reserva-se ao direito de monitorar e inspecionar todas as aplicações e dados localizados em seus ambientes de processamento e transmissão. Isto inclui, mas não é limitado, às mensagens de correio eletrônico, documentos de texto, gráficos e aplicações. Todas as aplicações e dados localizados nos equipamentos são considerados de propriedade da **OCB / SESCOOP**.

5. AÇÕES DISCIPLINARES

Qualquer usuário poderá, a qualquer tempo, ser auditado, através da Gerência de TI, para efeitos de verificação do descumprimento das normas e instruções corporativas e, em conseqüência, a aplicação de ações disciplinares cabíveis, a critério da chefia imediata, observada a sua gravidade, podendo ser censura, advertência, suspensão ou demissão.

A Gerência de TI fará auditorias periódicas, devendo comunicar à Superintendência Administrativa todas as ocorrências que necessitem de providências corretivas.

6. PADRONIZAÇÃO

A Gerência de TI padronizará a apresentação inicial dos computadores, tais como descanso de tela, papel de parede, formato de e-mail.

7. ATUALIZAÇÃO DESTA NORMA

A **OCB / SESCOOP**, por intermédio da Gerência de TI e da Superintendência Administrativa, reserva-se ao direito para modificar esta norma sempre que necessário.

8. CASOS OMISSOS

Os casos omissos serão levados à apreciação da Superintendência do SESCOOP/OCB, que deliberará sobre o assunto.

9. VIGÊNCIA

Esta norma entra em vigor a partir da data de sua assinatura.

Brasília, 03 de novembro de 2005.

SISTEMA OCB/SESCOOP

TERMO DE RESPONSABILIDADE

Pelo presente termo, declaro que li e entendi o conteúdo da presente norma e me comprometo em cumprir suas recomendações e determinações.
Declaro ainda que estou ciente da minha responsabilidade pelo uso indevido dos meios de informática, bem como qualquer desvio ou prejuízo causado por ato ou omissão de minha parte por desobediência às normas de segurança de informações da **OCB/SESCOOP**.

Nome do Funcionário
RG
CPF
Matricula

SAUS - Setor de Autarquias Sul, Quadra 04, Bloco I
CEP: 70070-936 - Brasília/DF
Telefone: (0xx61) 325-5500 Fax: (0xx61) 325-8383
email: ocb@ocb.org.br