PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Documento de Diretrizes e Normas Administrativas

OUTUBRO 2019

Histórico de revisão do documento:

28/10/2019	Publicação inicial, revisado por Daniela Bastos Martins e Julian Romero. Documento aprovado pela Diretoria e Presidência da CBDA. Conteúdo baseado em documento criado em 2016 pelo Departamento de TI da CBDA.

Sumário

Política de Segurança da Informação - PSI 3
Diretrizes 3
Objetivo 3
Aplicações da PSI 3
Princípios da PSI 3
Requisitos da PSI 4
Das responsabilidades Específicas 4
Dos Colaboradores em Geral 4
Dos Colaboradores em Regime de Exceção (temporários) 5
Dos Gestores de Pessoas e/ou Processos 5
Dos Custodiantes da Informação 5
1) Da Área da Tecnologia da Informação 5
2) Da Área de Segurança da Informação 6
Do Monitoramento e da Auditoria 7
Correio Eletrônico 7
Internet 8
Identificação 10
Computadores e Recursos Tecnológicos 11
Dispositivos Móveis 13
TI 13
BACKUP 13
Definições disposições finais 14
Anexo I – Modelo de Termo de Compromisso 15
Anexo II – Modelo de Termo de Confidencialidade 16

Política de Segurança da Informação
Diretrizes
A Política de Segurança da Informação, conhecida pela sigla PSI, é o documento de orientação que estabelece as diretrizes corporativas da **CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS – CBDA** para a proteção dos ativos de informação, a minimização de riscos do negócio, atendimento a requisitos legais e melhora da imagem da instituição junto à sociedade.
Deve, portanto, ser cumprida e aplicada em todas as áreas da Entidade.

Objetivos
Estabelecer diretrizes que permitam aos colaboradores e clientes da CBDA seguirem padrões de comportamento estabelecidos no ambiente corporativo e relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.
Difundir a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles internos e processos para seu atendimento.
Preservar as informações da **CBDA** quanto à:
Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
Confidencialidade: garantia de que o acesso à informação seja obtido somente através de pessoas e profissionais autorizados.
Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Aplicações da PSI
As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.
Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.
É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Princípios da PSI
Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela CBDA pertence à referida instituição. As exceções devem ser explícitas se formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.
A CBDA, por meio do departamento de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Requisitos da PSI
Para a padronização da informação, a PSI deverá ser comunicada a todos os colaboradores da CBDA e divulgada no sítio eletrônico da CBDA, a fim de que a política seja cumprida dentro e fora da empresa.
Periodicamente a PSI deve ser revisada e atualizada sempre que houver um fato relevante ou quando houver alteração nas Normas vigentes que regulam a sua implementação.
Deverá constar em todos os contratos da CBDA o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.
A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Devendo todos os colaboradores receber a orientação sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos e assinar um Termo de Responsabilidade e de Confidencialidade (Anexo II).
Todo incidente que afetar a segurança da informação deve ser comunicado imediatamente ao Departamento de TI, que ao analisar e julgar necessário, encaminhará à diretoria para análise e decisão.
A CBDA exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.
Esta PSI será implementada na CBDA por meio de procedimentos específicos, obrigatórios e padronizados para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.
O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

Das Responsabilidades Específicas

Dos Colaboradores em Geral
Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

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

Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê 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 o recebeu não estiver cumprindo as condições definidas no aceite.

Dos Gestores de Pessoas e/ou Processos

Servir de modelo de conduta para os colaboradores sob a sua gestão em relação à segurança da informação.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência (Anexo I), assim como a responsabilidade do cumprimento da PSI da CBDA em todos os seus termos estabelecidos.

Dos Custodiantes da Informação

1) Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a CBDA.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.
Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
Realizar auditorias periódicas de configurações técnicas e análise de riscos.
Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
Monitorar o ambiente de TI, gerando indicadores e históricos de:

- ✓ uso da capacidade instalada da rede e dos equipamentos;
- ✓ tempo de resposta no acesso à internet e aos sistemas críticos da CBDA;
- ✓ períodos de indisponibilidade no acesso à internet e aos sistemas críticos da CBDA;
- ✓ Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- ✓ Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

2) Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
Propor e apoiar iniciativas que visem à segurança dos ativos de informação da CBDA.
Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pela diretoria.
Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da CBDA, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
Analisar criticamente incidentes em conjunto com a diretoria da CBDA.
Buscar alinhamento com as diretrizes corporativas da instituição.

Do Monitoramento e da Auditoria
Para garantir as regras mencionadas nesta PSI, bem como de sua versão educacional, a CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS poderá:

- ✓ implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- ✓ tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- ✓ realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- ✓ instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Correio Eletrônico
O objetivo desta política é informar aos colaboradores da CBDA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.
O uso do correio eletrônico da CBDA é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique A CBDA e também não cause impacto no tráfego da rede.
A utilização de e-mails pessoais que não estejam vinculados a CBDA utilizando a rede cabeada é proibida.
Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da CBDA:

- ✓ enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;
- ✓ enviar 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;
- ✓ enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o CBDA ou suas unidades 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 as punições previstas;
- ✓ apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da CBDA estiver sujeita a algum tipo de investigação.
- ✓ produzir, transmitir ou divulgar mensagem que:

a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da CBDA;
b) contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
c) contenha 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;
d) vise obter acesso não autorizado a outro computador, servidor ou rede;
e) vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
f) vise burlar qualquer sistema de segurança;
g) vise vigiar secretamente ou assediar outro usuário;
h) vise acessar informações confidenciais sem explícita autorização do proprietário;
i) vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
j) inclua imagens criptografadas ou de qualquer forma mascaradas;
k) contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
l) tenha conteúdo considerado impróprio, obsceno ou ilegal;
m) seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
n) contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
o) tenha fins políticos locais ou do país (propaganda política);
p) 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:
Nome do colaborador
Gerência ou departamento
Nome da empresa
Telefone(s)
Correio eletrônico

Internet

Todas as regras atuais da CBDA visam basicamente o desenvolvimento de um comportamento ético e profissional do uso da internet.

Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a CBDA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet,

estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.
A CBDA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.
Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor.
O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.
A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.
Como é do interesse da CBDA que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.
Somente os colaboradores que estão devidamente autorizados a falar em nome da CBDA para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.
Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.
É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na CBDA e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela CBDA.
O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.
Qualquer software não autorizado baixado será excluído pelo departamento de TI.
Os colaboradores não poderão em hipótese alguma utilizar os recursos da CBDA para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.
Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.
Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a CBDA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da CBDA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.
O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos.

Identificação
Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante CBDA e/ou terceiros.
O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.
Todos os dispositivos de identificação utilizados na CBDA, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.
O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).
Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.
Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a CBDA e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.
É proibido o compartilhamento de login para funções de administração de sistemas.
O Departamento de Recursos Humanos da CBDA é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.
A TI da CBDA responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.
Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.
Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).
É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem

ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 5 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a TI da CBDA.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 60 (sessenta) dias, não podendo ser repetidas as 2 (duas) últimas senhas.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da CBDA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

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

As gerências que necessitarem fazer testes deverão solicitá-los previamente à TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da CBDA (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da CBDA e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da TI da CBDA ou por terceiros devidamente contratados para o serviço.

Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

O colaborador deverá manter a configuração do equipamento disponibilizado pela CBDA, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

Todos os recursos tecnológicos adquiridos pela CBDA devem ter imediatamente suas senhas padrões (default) alteradas.

Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da CBDA:

- ✓ Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- ✓ Burlar quaisquer sistemas de segurança;
- ✓ Acessar informações confidenciais sem explícita autorização do proprietário;
- ✓ Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- ✓ Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- ✓ Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- ✓ Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- ✓ Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Dispositivos Móveis

A CBDA permite a conexão de aparelhos moveis pessoais a internet por meio de sua conexão WIFI. Nesta conexão é permitido o uso de redes sociais, e-mails pessoais e outros sites, desde que com uso moderado e responsável.

A CBDA, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros,de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na CBDA, mesmo depois de terminado o vínculo contratual mantido com a instituição.

TI

O acesso ao departamento de TI é restrito. Apenas o colaborador do setor terá acesso às dependências.

O usuário "administrador" do sistema de autenticação ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

Quando não houver colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup”– períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível da empresa.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.
Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.
É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.
As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, distante no mínimo 10 quilômetros da empresa.
Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.
Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.
Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.
Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backupe Restore.
Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

Das disposições finais

O comprometimento com a ética e a participação de todos os usuários da CBDA com a Política de Segurança da Informação se faz necessário para um maior controle e minimização dos riscos do negócio, primando pela excelência das atividades e melhorando a imagem da Entidade junto à sociedade.

ANEXO I

MODELO DE TERMO DE COMPROMISSO

Declaro que tenho pleno conhecimento da Política de Segurança de Tecnologia da Informação definida nos termos de sua atualização em Outubro/2019, publicada e disponibilizada no sitio eletrônico da CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS.

Declaro estar ciente de que atos contrários à Política de Tecnologia da Informação poderão resultar na aplicação de medidas administrativas, inclusive na rescisão do contrato de trabalho ou de prestação de serviços, bem como na aplicação de medidas judiciais pertinentes.

Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência de meu vínculo contratual com a CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS - CBDA, mesmo após o seu encerramento.

Rio de Janeiro, ___ de _____ de _____.

DADOS DO EMPREGADO

Nome:

CPF:

RG.:

DADOS DO PRESTADOR DE SERVIÇO/PARCEIRO

Nome:

CPF:

Unidade de Ação:

Nome da Empresa:

CNPJ:

Endereço Comercial:

Telefone Com.: ( ) Ramal:

E-mail:

Nome do gestor do contrato:

E-mail:

ANEXO II

MODELO DE TERMO DE CONFIDENCIALIDADE

Pelo presente termo, (NOME DA EMPRESA), com sede (ENDEREÇO COMPLETO: CEP. CIDADE, ESTADO), inscrita no CNPJ sob o nº (00.000.000/0000-00), neste ato representada conforme seu contrato social, doravante denominada "PRESTADORA", assume o compromisso irrevogável e irretratável de manter o mais absoluto sigilo em relação a todas as informações que lhe forem disponibilizadas pela CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS, sob qualquer forma, para o desenvolvimento dos serviços contratados.

As informações conferidas à PRESTADORA não poderão ser divulgadas, tampouco acessadas por pessoas não autorizadas, mesmo após finalizada a prestação de serviços.

A PRESTADORA deverá indenizar a CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS por perdas e danos sofridos em decorrência da falha de manutenção de sigilo por parte de seus empregados, bem como de qualquer pessoa à qual tenha dado indevidamente acesso às informações confidenciais.

As informações disponibilizadas pela CONFEDERAÇÃO BRASILEIRA DE DESPORTOS AQUÁTICOS deverão ser restituídas imediatamente assim que requerido, juntamente com quaisquer cópias eventualmente realizadas.

Rio de Janeiro, ___ de _____ de _____.

_____

(NOME DO RESPONSÁVEL)

(NOME DA EMPRESA)

Testemunhas:

1.

2.