Normativo de Tecnologia da Informação

1. OBJETIVO

Normatizar as regras e procedimentos que se relacionam com o âmbito da tecnologia da informação na Confederação brasileira de Rugby (CBRu).

2. ÁREAS APLICÁVEIS

Esse Procedimento se aplica a todos responsáveis pela tecnologia da informação da Confederação brasileira de Rugb (CBRu), bem como as demais áreas presentes na confederação.

3. ASPECTOS GERAIS

Os aspectos referentes aos controles internos tratados nesta política poderão ser objeto de auditoria quanto à sua efetiva aplicação e eficácia. A violação da política de segurança de TI pode levar a suspensão temporária e até definitiva do acesso do usuário aos recursos de TI a ele disponibilizados, e a sanções em conformidade com a legislação trabalhista e normas internas da CBRu.

São obrigações das áreas da CBRu em relação a esta política:

- Gerência:

  a) Validar as propostas de revisão desta Política, visando contínua adequação e eficácia dos controles implementados;

  b) Autorizar providências para obtenção dos recursos necessários para o cumprimento da política de segurança de TI;

  c) Promover o desenvolvimento da cultura de segurança de TI junto aos usuários sob sua responsabilidade e zelar pelo seu cumprimento.

- Usuários:

  a) Zelar pelos recursos de TI (equipamentos, sistemas aplicativos e softwares) sob sua responsabilidade ou que venha a ter acesso;

  b) Proteger todas informações às quais tenha acesso e responsabilidade;

c) Relatar qualquer situação relacionada ao uso dos recursos de TI, que possam prejudicar a continuidade ou negócio da CBRu.

- Área de TI:

a) Zelar pela disponibilidade dos recursos de TI de modo a não gerar atrasos ou prejuízos em nenhum processo, garantindo a não descontinuidade das operações pelos usuários da CBRu;

b) Envidar esforços na busca de soluções nas interrupções procurando eliminar ou minimizar ao máximo os prejuízos à operação;

c) Monitorar e implementar os processos de controle e operação propostos nesta política garantindo sua atualização e proteção quanto ao uso inadequado dos recursos de TI, mudanças na legislação e/ou nos requisitos do negócio.

4. DOS CONTROLES DE ACESSO

Todo cadastro de usuário será mantido em sistema ou aplicação e deverá possuir, no mínimo, os seguintes campos:

1) Nome completo do usuário;
2) Tipo de usuário, que poderá ser: (a) colaborador(a), (b) estagiário(a), (c) prestador(a) de serviço, (d) auditor(a), (e) consultor(a) ou (f) assistido(a);
3) Código para acesso vinculado ao identificador do usuário (ID autorizador);
4) Perfil do usuário: servirá para identificar as funcionalidades as quais o usuário terá acesso ou poderes de modificação, podendo ser:

I - Gerente/Administrador;

II - Operador;

5) Identificação do solicitante de cadastramento: chave do solicitante será registrada junto ao cadastro criado;
6) Data de criação do usuário: ao realizar o cadastro, a data de criação deverá ser armazenada;
7) Motivo da criação do usuário, que poderá ser:

(a) Admissão;

(b) Contratação;

(c) Autorização;

8) Data de bloqueio do usuário: ao realizar o bloqueio do usuário a data deverá ser registrada;

9) Informação de razão de bloqueio:

(a) Férias,

(b) Demissão,

(c)Término de contrato,

(d) Desautorização de uso;

10) Data da última atualização de dados cadastrais do usuário: identificação do último responsável pela atualização dos dados cadastrais do usuário.

5.DOS SISTEMAS DESENVOLVIDOS OU ADQUIRIDOS

Os sistemas aplicativos desenvolvidos ou adquiridos devem permitir, minimamente:

1. Customizações de senhas:

b) Definição de tempo para bloqueio/expiração de contas e/ou senhas;

c) Definição do número máximo de tentativas de acesso incorretas consecutivas com bloqueio de contas e/ou senhas. Sendo que este deverá ser configurado conforme abaixo:

i. A senha deverá ter o mínimo de 08 (oito) caracteres;

ii. Considerando 04 (quatro) tipos de caracteres (letras minúsculas, letras maiúsculas, números e símbolos), a senha deve ser composta de pelo menos 3 (três) tipos;

iii. O número máximo de tentativas de autenticação sem sucesso nos sistemas (logon) é 03 (três) vezes. No caso deste número ser ultrapassado, a conta do usuário irá permanecer bloqueada, sendo a liberação efetuada apenas por solicitação formal do superior direto ao responsável pela TI;

iv. As senhas de acesso terão uma validade de 120 (cento e vinte) dias, sendo requisitada automaticamente a sua troca para o usuário;

v. O usuário não poderá reutilizar as suas últimas 05 (cinco) senhas.

2. Controlar o acesso de forma uniforme, utilizando uma única rotina de verificação e gerenciamento centralizada:

Normativo de Tecnologia da Informação

a) Os usuários deverão ter acesso concedido apenas através de perfil, e nenhum usuário poderá ter mais de um perfil;

b) A autorização para utilização de cada função, tela ou módulo do sistema aplicativo deverá ser realizada por usuário, e deverá ser solicitada à equipe de TI através de e-mail, aprovada pela Gerência ou Diretoria;

c) Rotinas que necessitem de ações de um único usuário (ex. aprovações financeiras), o sistema deve permitir delegação de função de maneira a não comprometer as atividades em caso de ausência deste, solicitada à equipe de TI através de e-mail, com aprovação da Gerência.

3. Permitir o bloqueio de acesso ao sistema aplicativo de forma automática, ou manual, quando da ausência temporária do usuário por motivo de férias, licença ou por motivos de força maior.
4. Todo acesso a sistemas aplicativos deverá ser realizado através de identificação de usuário individualmente e autenticação através de senha. É de responsabilidade do usuário os cuidados com a manutenção de segurança e sigilo da senha, evitando sua utilização indevida: "As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese."
5. Os desenvolvedores devem ter acesso apenas às fontes necessárias à execução do seu trabalho.
6. As contas com privilégios administrativos das bases de dados serão concedidas apenas para a equipe de TI, com assinatura do "Termo de responsabilidade de Acesso e Concessão de Acesso ao Banco de Dados da CBRu".
7. A reinicialização de senha deve ser solicitada à equipe de TI, de forma autorizada pela Gerência, através de e-mail. Será criada uma senha expirada (com obrigatoriedade de troca no primeiro acesso), que a equipe de TI enviará diretamente ao usuário, preferencialmente, através de e-mail.
8. Os sistemas desenvolvidos ou adquiridos pela CBRu não devem utilizar contas administrativas ou privilegiadas de sistemas operacionais, servidores web ou banco de dados.

Normativo de Tecnologia da Informação

9. O sistema, ou a rede à qual estiver utilizando, deverá desconectar o usuário por tempo de inatividade superior a 15 (quinze) minutos.
10. Nos casos em que a aplicação necessite estar conectada diretamente à internet, esta deverá estar segregada física e/ou logicamente da rede corporativa e protegida por mecanismo de detecção e prevenção de intrusos, em rede própria ou terceirizada.
11. Os desenvolvedores e testadores devem ser autenticados lógica e fisicamente ao acessar os ambientes de desenvolvimento e homologação. Não é permitido, mesmo nestes ambientes, acesso não identificado ou com conta genérica.
12. A extração da base de dados deve ser efetuada pela área de TI e com autorização formal da Diretoria, com o objetivo de evitar o vazamento de informações.

6. DA SEGURANÇA DA INFORMAÇÃO

Os sistemas que utilizam informações confidenciais deverão utilizar mecanismos criptográficos para a proteção destas.

Este procedimento se aplica, principalmente, às transmissões eletrônicas de dados executadas para bancos, patrocinadoras, auditorias e consultorias contratadas. Os sistemas que estiverem disponíveis na internet e trafeguem informações confidenciais deverão utilizar mecanismos de autenticação para a segurança e proteção.

Este procedimento aplica-se aos softwares utilizados para acesso e simulações disponibilizadas pela CBRu aos usuários Os sistemas cujas informações estiverem expostas ao risco de perda de integridade deverão utilizar mecanismos de verificação para a sua proteção. Este procedimento se aplica aos softwares utilizados para o envio de mensagens ou arquivos anexados.

7. DA AUDITORIA E MONITORAMENTO ELETRÔNICO

Todos os sistemas desenvolvidos ou adquiridos pela CBRu devem conter registros de auditoria (logs). Estes registros devem ser gravados com data/hora de ocorrência, endereço, IP e host name (endereço da estação de trabalho), conta utilizada e deve registrar, minimamente, os seguintes eventos:

Normativo de Tecnologia da Informação

1) Falhas de acesso nos sistemas;
2) Acessos e alterações em dados confidenciais utilizados pelos sistemas;
3) Criação e a remoção de usuários;
4) Atribuição e remoção de direitos e acessos do usuário.

Deverá haver uma interface amigável para consulta dos logs. Todos os logs devem ser protegidos, cabendo apenas, usuários com perfis específicos e restritos, o acesso e a possível deleção dos dados.

Os registros devem ser desenvolvidos e configurados de forma a evitar a exaustão da trilha de auditoria. Os logs devem ser mantidos por períodos mínimos determinados pelos gestores, devendo considerar os aspectos legais e regulatórios envolvidos, bem como as necessidades de negócio.

Recomenda-se, nos casos omissos, a manutenção destes por um período não inferior a 5 anos

8. DOS TESTES E HOMOLOGAÇÃO

Todo sistema desenvolvido ou adquirido pela CBRu deve ser testado e homologado antes de ser colocado em produção. Estes testes devem contemplar no mínimo:

1) Validação de todas as entradas de dados (de usuários ou interface com outros sistemas) quanto a formato dos dados e valores/caracteres esperados.

2) Implementação de funcionalidades de segurança, incluindo todas as condições definidas neste documento. Todo sistema desenvolvido ou adquirido pela CBRu deve garantir que:

1) Os arquivos e componentes desnecessários para o funcionamento do sistema aplicativos sejam removidos no ambiente de produção.

2) As bibliotecas e componentes externos usados no sistema aplicativo sejam homologados previamente

9. DA DOCUMENTAÇÃO

Todo sistema desenvolvido ou adquirido pela CBRu deverá possuir manual de administração, contendo:

1. Procedimentos de instalação que contenham, no mínimo:

a) Itens de verificação do ambiente antes da instalação;

b) Definições de configuração e primeiro uso.

2) Procedimentos de segurança que contenham, no mínimo:

a) Informações para recuperação em casos de erro, falha ou incidente;

b) Definições sobre atualização, backup, auditoria e monitoramento (caso não atendam ao padrão estabelecido pela área de TI).

10. MANUTENÇÃO E AQUISIÇÃO DE EQUIPAMENTOS E SISTEMAS

Todas as solicitações de manutenção, nos sistemas aplicativos existentes, e de desenvolvimento de novos sistemas e funcionalidades, deve estar em conformidade com a "Norma para Requisição de Desenvolvimento e Manutenção de Prioridades de Solicitações de Serviço de TI".

O Ambiente de produção deve ser corretamente configurado e constantemente atualizado, de forma a manter segura a camada subjacente ao sistema, evitando falhas que possam invalidar os mecanismos de segurança implementados, ou permitir diversos tipos de ataque ou erros de utilização.

Fica a equipe de TI responsável pela elaboração de regras de backup dos servidores, bancos de dados, sistemas aplicativos, áreas de dados pessoais e Política de Tecnologia da Informação Normativos e Divulgações – Padrões corporativos, para os casos da rede de dados e os equipamentos serem de propriedade da CBRu, das patrocinadoras ou terceirizados. No caso de utilização da rede das patrocinadoras, ou terceirizada, a regra de backup poderá vir a ser adotada a mesma regra praticada pela proprietária da rede, desde que esteja em conformidade às melhores práticas de segurança definidas nesta Política.

A área de TI deverá prover e gerir contratos de manutenção para os servidores de propriedade da CBRu na modalidade 24x7 (24 horas por dia e 7 dias da semana) com cobertura contratual total para:

1) Sobreaquecimento do servidor;

2) Danos nas fontes, na placa mãe, no processador, na memória, nos discos rígidos, na placa de rede etc.

A área de TI deverá atuar junto à Diretoria no planejamento e na execução orçamentária para atualização dos equipamentos de TI de propriedade da CBRu. As estações de trabalho e notebooks

devem ser substituídas anualmente na proporção de até 30% (trinta por cento) da quantidade total instalada. A área de TI deverá realizar estudos para atualização dos servidores de propriedade da CBRu, e apresentar o relatório à Diretoria para avaliação e inserção no planejamento orçamentário anual, considerando:

1) Performance do servidor;
2) O nível de manutenção existente X tempo de vida útil do equipamento;
3) Adequação de espaço em disco para utilização pelos sistemas e usuários no desenvolvimento de suas atividades.

Os equipamentos a serem adquiridos devem ser homologados e estar de acordo com os parâmetros operacionais exigidos para instalação na rede da CBRu. O processo de compra deve ser gerido pela área específica da CBRu, com alinhamento direto com a Gerência Administrativa-Financeira.

11. DA TERCEIRIZAÇÃO DE SERVIÇOS

O desenvolvimento terceirizado de sistemas deve ser realizado em conformidade com os controles definidos neste regulamento de segurança da informação.

O desenvolvimento terceirizado de sistemas deve ser monitorado constantemente, através da implementação de procedimentos específicos, tais como:

1) Inclusão de termos sobre licenças, propriedade de código-fonte, direitos de propriedade intelectual e confidencialidade de informações nos contratos e acordos de nível de entrega dos serviços de terceiros.
2) Certificação da qualidade e a exatidão do trabalho implementado.
3) Definição de sanções ou ações específicas para a eventualidade de falha por parte dos prestadores de serviço.
4) Garantia de direitos de acesso para auditoria da qualidade e exatidão do trabalho executado.
5) Definição de requisitos contratuais de qualidade e de segurança

12. DO CATÁLOGO DE SERVIÇOS DE TI

Normativo de Tecnologia da Informação

A CBRu deve manter organizado um catálogo publicado e atualizado dos serviços de TI, incluindo os níveis de serviços. Esta publicação deve ser atualizada trimestralmente, sendo uma atribuição da empresa de TI.

13.DA INTEGRAÇÃO DOS PROJETOS DE TI COM A ESTRATÉGIA ORGANIZACIONAL

Todos os projetos de tecnologia devem estar integrados com a estratégia da CBRu, dando preferência para soluções que colaborem ou otimizem o alcance de resultados.

Assim, todos os projetos de TI devem estar associados a objetivos estratégicos e respectivo mapa estratégico da CBRu.

14.DA RESPONSABILIDADE PELO USO DE DISPOSITIVOS DE PROPRIEDADE PESSOAL

As regras e dispositivos desta política se destinam aos colaboradores e prestadores de serviços da CBRu que se utilizam de dispositivos de propriedade pessoal para o exercício de suas atividades profissionais.

Considera-se Dispositivos de Propriedade Pessoal (DPP) os laptops, tablets, PCs ultra-móveis (UMPCs), PCs de mesa (desktop), palmtops, telefones celulares, smartphones, câmeras digitais, registros de notas digitais, impressoras e outros que se enquadrem em características similares. Soma se, ainda, as mídias de armazenamento portátil, como cartões de memória USB, cartões de memória, discos rígidos portáteis (HD externo), disquetes, pen drives ou outros.

Os(As) colaboradores(as) que optarem, voluntariamente, por utilizar DPP para fins de trabalho, devem ser explicitamente autorizados a fazê-lo por um superior imediato.

A proteção aos dados corporativos deve ser salvaguardada na mesma medida que em equipamentos de Tecnologia da Informação e Comunicação (TIC) de propriedade da organização e não devem apresentar riscos indesejáveis (como malware, vírus ou outros) nas redes e demais equipamentos de propriedade da entidade e em uso por outros colaboradores.

Normativo de Tecnologia da Informação

Esta política faz parte dos pressupostos de governança corporativa estabelecidos pela CBRu. É, particularmente, relevante para os funcionários que desejam usar os DPP para fins de trabalho.

Esta política também se aplica a terceiros que atuem em um formato similar ou não aos funcionários da CBRu, quando em período de prestação de serviços para a entidade.

Em contraste com os dispositivos de TIC de propriedade da organização, os DPPs são dispositivos de TIC de propriedade de funcionários ou de terceiros (como fornecedores, consultorias e prestadores de serviços de manutenção ou operação de eventos). Funcionários autorizados e terceiros podem usar seus DPPs para fins de trabalho. Por exemplo, fazer e receber chamadas telefônicas e mensagens de texto em seus próprios telefones pessoais, usando seus próprios tablets para acessar, ler e responder a e-mails ou trabalhar em regime de trabalho remoto (home-office).

O ingresso de DPPs está associado a vários riscos de segurança da informação, tais como:

- Perda, divulgação ou corrupção de dados corporativos em DPPs;
- Incidentes envolvendo ameaças ou comprometimento da infraestrutura de TIC corporativa e outros ativos de informação (por exemplo, infecção por malware ou invasão de hackers);
- Não-conformidade com leis, regulamentos e obrigações aplicáveis (por exemplo, privacidade ou pirataria);
- Direitos de propriedade intelectual para informações corporativas criadas, armazenadas, processadas ou comunicadas em DPPs durante o trabalho da organização.

Devido às preocupações da entidade com relação aos riscos de segurança da informação associados, os indivíduos que desejarem aderir a esta política devem ser autorizados pelo seu superior imediato e devem aceitar explicitamente os pressupostos ora estabelecidos.

Ao superior imediato é reservado o direito de não autorizar indivíduos, ou de retirar a autorização, se considerar que há riscos iminentes à segurança da informação ante os interesses organizacionais.

Normativo de Tecnologia da Informação

A CBRu deve manter o fornecimento, a sua escolha, de dispositivos de TIC totalmente proprietários e gerenciados por ela, conforme suas necessidades, para fins de se realizar regularmente as atividades pelas quais o funcionário foi contratado.

A organização e os proprietários e usuários de DPPs compartilham responsabilidades pela segurança da informação.

Nada nesta política afeta a propriedade da organização sobre informações corporativas, incluindo toda a propriedade intelectual relacionada ao trabalho criada no decorrer do trabalho em DPPs.

O funcionário tem a obrigação de, ao criar documentos e/ou gerar informações em DPPs, quando relacionados com suas atividades laborais, de inseri-las regularmente (ao menos uma vez ao mês) ou automaticamente, nos servidores físicos e/ou em nuvem disponibilizados pela entidade.

Os dados corporativos só podem ser criados, processados, armazenados e comunicados em dispositivos pessoais que executam o(s) software(s) escolhidos pela entidade.

Dispositivos que não executam um ou mais softwares oficiais, ou aqueles em que os proprietários de DPPs se recusem a autorizar que a área de TIC os instale, não poderão ser utilizados para fins de atividade oficial.

Os DPPs devem usar formas apropriadas de autenticação de dispositivo aprovadas pela área de TIC, como os certificados digitais criados para cada dispositivo específico. Os certificados digitais não devem ser copiados ou transferidos entre os DPPs.

Os usuários optantes por seguir esta política devem utilizar formas apropriadas de autenticação do usuário aprovadas pela área de TIC da entidade, como userlDs, senhas e/ou outros dispositivos de autenticação, conforme cada necessidade.

As seguintes classes ou tipos de dados corporativos não são adequados a esta política e não são permitidos em DPPs:

- Qualquer informação ou arquivo classificado como “Secreto” ou classificação análoga;
- Outras informações corporativas atualmente não confidenciais, mas que sejam altamente valiosas ou sensíveis, que provavelmente serão classificadas futuramente como “Secreta”;

Normativo de Tecnologia da Informação

- Grandes quantidades de dados corporativos (ou seja, mais de 1 Gb em agregação em qualquer DPP ou dispositivo de armazenamento).

A CBRu tem o direito de controlar suas informações. Isso inclui o direito de fazer backup, recuperar, modificar, determinar o acesso e/ou excluir dados corporativos sem referência ao proprietário ou usuário do DPP.

A organização tem o direito de apreender e realizar exame forense de qualquer DPP que contenha ou possa conter dados corporativos, quando necessário, para fins de investigação ou controle.

Um software antivírus adequado deve ser instalado e executado corretamente em todos os DPPs.

Os usuários de DPPs devem garantir que os dados corporativos criados ou modificados nos DPPs sejam armazenados em backup regularmente, ao menos mensalmente ou automaticamente, de preferência conectando-se à rede corporativa e sincronizando os dados entre o DPP e uma unidade de rede. Ou em mídia removível armazenada com segurança.

Qualquer DPP usado para acessar, armazenar ou processar informações confidenciais deve criptografar dados transferidos pela rede (por exemplo, usando SSL ou VPN) e armazenados no DPP ou em mídia de armazenamento separada, qualquer que seja a tecnologia de armazenamento usada (por exemplo, disco rígido, disco de estado sólido, CD / DVD, USB / cartão de memória flash, disquete etc.).

Uma vez que a área de TIC pode não ter recursos ou tempo adequado para oferecer suporte a todos os dispositivos e softwares possíveis, os DPPs poderão receber suporte limitado em uma base de “melhores esforços”, sem obrigatoriedade de fornecimento de serviços em prol destes usuários.

Embora os funcionários tenham uma expectativa razoável de privacidade sobre suas informações pessoais em seus próprios equipamentos, o direito da organização de controlar seus dados e gerenciar DPPs pode, ocasionalmente, fazer com que a área de suporte tenha acesso não intencional às informações pessoais. Para reduzir a possibilidade de tal divulgação, os usuários de DPPs são aconselhados a manter seus dados pessoais separados dos dados ligados à entidade no DPP, em

Normativo de Tecnologia da Informação

diretórios separados, nomeados de forma clara e dentro dos padrões estabelecidos pela própria entidade.

É vedado o uso de DPPs que possam infringir os direitos de privacidade de outras pessoas no ambiente de trabalho.

A área de TIC é responsável por manter essa política e aconselhar sobre os controles de segurança da informação. É, ainda, responsável pela emissão de certificados digitais para autenticar DPPs autorizados e para monitorar a segurança da rede para acesso não autorizado, tráfego de rede inadequado, dentre outros etc. Deve trabalhar em conjunto com outras funções corporativas, sendo responsável pela execução de atividades educacionais para aumentar a conscientização e compreensão das obrigações de todos os usuários atinentes a esta política.

A área de TIC é responsável por gerenciar a segurança dos dados corporativos e configurar a segurança em DPPs autorizados. É, também, explicitamente responsável por garantir a segurança de software e para procedimentos relacionados a fim de minimizar o risco de invasão de hackers, que possam explor o sistema para acessar dispositivos móveis.

Os funcionários e prestadores de serviço (quando aplicável), são responsáveis pelos seus DPPs em relação a sua manutenção, armazenamento, transporte e utilização. A CBRu se exime de quaisquer responsabilidades quanto à danificação ou redução da vida útil de um ou mais DPP no ambiente de trabalho desta.

A CBRu se exime, ainda, de responsabilidades em caso de furto, roubo, perda ou dano irreparável, causado pelo próprio funcionário ou prestador de serviço ou por terceiros. Por isso, a entidade não reconhece a sua responsabilidade em repor, de forma parcial e/ou integral, DPPs que, porventura, tenham registrado intercorrência em suas dependências ou a serviço para esta.