POLÍTICA DE GESTÃO DE ACESSOS E IDENTIDADES

Autores: Dual Tech Informática

Data de Criação: 10/08/2022
Última Atualização: 30/08/2022
Versão: 1.0

Registro de Alterações

Data	Autor	Versão	Descrição
14/06/2022	Bruno Fausto	1	Implantado o domínio no servidor, criado os usuários e reconfigurado o acesso as pastas mapeadas no servidor.
30/07/2022	Bruno Fausto	1	Efetuada a implementação do Active Diretory em todas as máquinas dos colaboradores.

Revisores

Descrição	Nomes

Nota:

Este documento contém informações confidenciais e sigilosas. Não divulgue ou compartilhe, sem uma autorização formal para esta ação.

Qualquer dúvida, entre com contato com os responsáveis.

Observação:

Este documento está sujeito ao instrumento Licença e Termo de Usos do PACOTE LGPD

Sumário

Escopo

Demonstrar como as identidades e acessos na empresa devem ser gerenciadas de forma adequada e segura.

Objetivo

O objetivo principal é apresentar as medidas organizacionais para gerenciar e organizar o acesso às informações e estabelecer os requisitos necessários para gerenciamento de acessos dos usuários na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA.

A quem se destina

Privada: Deverá ser implementada internamente e revisa pelo comitê de segurança e/ou de privacidade e proteção de dados e o Encarregado(a) de Privacidade e Proteção de Dados (DPO) responsável.

Referências

- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.
- Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H. Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002. Brasport, 1ª edição, 2018.
- LEI GERAL DE PROTEÇÃO DE DADOS – LEI 13.709/18
- PROJETO ABNT PE-451.01 - Certificação de Sistemas de Gestão da Proteção e Privacidade de Dados Pessoais
- PROJETO ABNT NBR ISO/IEC 27001
- PROJETO ABNT NBR ISO/IEC 27701

Política de Gestão de Acessos e Identidades

Introdução

Seja bem-vindo(a) a nossa política de gestão de acessos e identidades. Nesta política, vamos apresentar as medidas organizacionais para gerenciar e organizar o acesso à informação e estabelecer os requisitos necessários para gerenciamento de acessos dos usuários na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA
Esta política visa proteger a confidencialidade, integridade e disponibilidade das informações na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA e leva em consideração a cultura organizacional e medidas técnicas.

Identificação, autenticação e autorização

Os requisitos para estabelecer os controles de acesso na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, devem levar em consideração as etapas:

Na identificação deve ser a primeira etapa para concedermos os acessos, nossos usuários devem apresentar seu nome de usuário/senha. Lembrando que o usuário e senha **deve ser único e intransferível**, não deve ser compartilhado em hipótese alguma com outras pessoas!
Jamais devemos salvar a senha em post-its, blocos de notas, ou arquivos em Excel, repositórios compartilhados e outros. Todos os colaboradores devem ser responsáveis por manter as suas credenciais seguras! Em caso de dúvida, devem entrar em contato com o time de segurança (13) 4042-0997 telefone/whatsapp.

Nossos sistemas devem verificar se a senha é válida e quais recursos o acesso pode ser concedido, de acordo com o perfil e as autorizações, que serão permitidas ou negadas, de acordo com cada grupo.

- Devemos levar em consideração para a autorização: os requisitos de negócio, classificação das informações, as tarefas realizadas, sistemas que a conta será aprovisionada e tipos de acessos.

- Sobre os direitos de acesso: O que podemos acessar e o que podemos fazer, são baseados nas nossas atividades de negócios, orientados por dois princípios:

  a) **necessidade de conhecer:** somente tem permissão para acessar informação que necessita para desempenhar as tarefas (nada à mais que isto, para tarefas e atribuições diferentes significam diferentes perfis de acesso);
  b) **necessidade de uso:** somente tem permissão para acessar os recursos de processamento da informação (equipamentos, aplicações, procedimentos etc.), quem necessita para desempenhar a tarefa/função/papel.

Pontos de atenção para gestão de acessos

Aqui na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, devemos tomar todos os cuidados na especificação de regras de controle de acesso:

a) Seguimos o seguinte mantra: *"**Tudo é proibido a menos que expressamente permitido**";*
b) mudanças na classificação das informações e mudanças em permissões de usuário e de regras, requerem um fluxo aprovação específico;

As solicitações de acessos e mudanças de privilégios devem ser registradas e acionadas por um fluxo de aprovação, que passe pelo menos: aos controles do gestor do colaborador e o responsável pelo sistema.

O fluxo de solicitação funcionara da seguinte forma:

- Abertura de chamado com a Dual Tech Informática;
- A solicitação será analisada, e caso esteja dentro do escopo pré-aprovado entre Dual Tech Informática e a Diretoria do Grupo Bortone, será realizado;
- Caso a solicitação esteja fora do escopo, será repassada para a Diretoria do Grupo Bortone, e o chamado será atendido ou rejeitado;

Gerenciamento de acesso do usuário

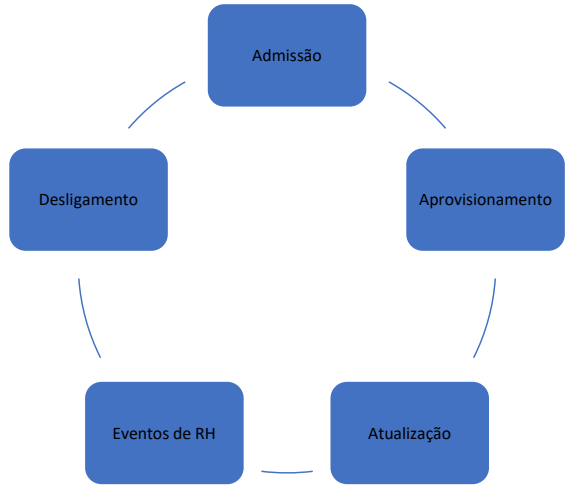
- Deve-se assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços. Para isto, os procedimentos de controle de acesso devem ser implementados, documentados, revisados de acordo com a estrutura da BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA e mantidos atualizados para cada sistema que for utilizado.

- Deve ser levado em consideração do ciclo de vida da identidade do colaborador: desde a admissão, atualização, promoção, licenças, férias e até o cancelamento/desligamento, quando os acessos devem ser desativados e posteriormente, eliminados.

- Atenção redobrada para os acessos de administração, e privilegiados, deverão ser fornecidos apenas para colaboradores que autorizados e que tenham os privilégios necessários, para executar as atividades de administração de sistemas. Da mesma forma, devemos evitar ao máximo as contas de administração genéricas e sempre que possível, tornar nominal, para termos rastreabilidade das atividades executadas.

Gestão da Identidade

Ao realizar uma admissão, devemos ter uma *identidade* como colaborador criada na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, considerando apenas as informações necessárias para criar as contas de acesso para utilizar os sistemas da BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA: nome, contatos, matrícula, cargo, área, gestor e outros. Desta forma, a identidade deve ser estabelecida conforme ciclo de vida abaixo:



- Admissão: Dados coletados no processo de admissão pelo RH;
    - Assim que uma admissão é realizada o time de RH do Grupo Bortone, deve informar o time da Dual Tech, solicitando a criação de um novo usuário para acesso ao domínio, fornecendo o nome e sobrenome do novo colaborador (deverá ser aberto um chamado com a equipe da Dual Tech Informática);

- Aprovisionamento: Sistemas em que o colaborador terá a conta criada, com os devidos privilégios, somente o necessário para realizar as atividades, de acordo com o perfil estabelecido;

- Atualização: As suas informações do colaborador podem ser atualizadas, tais como: nome, cargo, endereço, telefone e outros;

- Eventos de RH: Os eventos de férias, afastamento, promoção, mudança de área, licenças e outros, devem impactar diretamente nas atualizações das suas contas: desabilitação de privilégios, ajustes de acessos, módulos novos e outros. As

contas durante o período de férias e afastamento, devem permanecer bloqueadas, conforme instruções do RH, em caso de dúvidas procure pelo time da Dual Tech informando o colaborador a ser bloqueado.
    - Em caso de mudança de cargo ou promoções, os acessos não devem ser herdados de outra pessoa, ou seja, espelhados/copiados. Deve ser verificado sempre o perfil correspondente e somente fornecidos os acessos necessários, que devem passar pelo fluxo formal de aprovação;

- Desligamento: Cancelamento/desabilitação das contas de acessos.
    - Os desligamentos e cancelamentos de contrato, devem ser informados imediatamente pelo gestor responsável e acionado o time de segurança da Dual Tech, para desativação das contas e acessos correspondentes.

Aprovisionamento e desligamento

As contas criadas no processo de admissão e novas solicitações, sejam para acesso a rede ou nos sistemas, devem primeiramente serem enviadas aos cuidados do gestor responsável para aprovação. Qualquer novo acesso, deverá ser solicitado formalmente, passar por um processo de verificações de segurança e autorização, para que sejam criadas as contas e privilégios.

O controle eficaz requer que atividades e áreas de responsabilidades conflitantes, sejam segregadas, para reduzir o risco de um acesso não autorizado a um ativo ou uma modificação ou mau uso não intencional.

- Quando um colaborador é desligado da BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA ou um terceiro tem um contrato encerrado, as contas de e-mail e acessos ao domínio são inativadas, bem como as demais, que possa ter acesso;
- É fundamental que no desligamento ou encerramento de contrato, todas as contas sejam desativadas para evitar o acesso não autorizado.

DÚVIDA
O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;
- Mudança de função do colaborador;
- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
- Para os cancelamentos acima mencionados, o Departamento de Recursos Humanos ficará responsável por informar prontamente os responsáveis acerca dos desligamentos e mudança de função dos colaboradores.

Em cenários que possa haver o risco de um funcionário ou terceiro querer prejudicar a BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, devemos adotar procedimentos adicionais para remover o acesso, antes da notificação

de desligamento, entre em contato com o departamento de RH do Grupo Bortone e envolva o time de segurança da Dual Tech Informática.

- As contas de acesso não devem ser reutilizadas. O colaborador que for desligado e retornar para a BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, deve retornar com outro acesso.

Atualizações, revisões e acessos privilegiados

- Mudanças de perfis de acessos, alterações de cargo, mudanças de áreas e novos direitos de acessos, devem passar por um processo formal de aprovação do gestor, via chamado em nosso portal de atendimento pelo whatsapp (13) 4042-0997;

- Não é permitido que um administrador ou usuário com acesso privilegiado, ajuste seus próprios acessos e direitos, sem que haja a aprovação formal de seus gestores;

- Acessos privilegiados como administradores devem ser criados e identificados para cada sistema target ou rede, sob rígidos controles associados a contas de nível de administrador. Essas contas devem ser específicas para cada colaborador: "*ex: maria_silva*". Contas genéricas devem ser evitadas ao máximo pois não fornecem o nível de rastreabilidade necessário e não identificam os usuários;

- Direitos de acesso de nível administrador devem ser atribuídos apenas a colaboradores que possam exercer tais funções com respectivos conhecimentos, responsabilidades, conhecimentos, experiências, treinamentos e habilidades correspondentes.

Deve ser implementado um processo de revisão de acessos regularmente, pelo menos semestralmente, para garantir que os acessos estão adequados às responsabilidades e funções desempenhadas. É importante incluir na revisão:

- Contas dos ex-colaboradores e terceiros, que foram desligados;
- Colaboradores que poderiam ter eventualmente algum acesso às contas compartilhadas como por exemplo "monitoramento@..., contasapagar@...". Relembrando que contas genéricas ou compartilhadas, devem ser evitadas ao máximo!
- Contas com excesso de direitos/privilégios;
- Contas que estão genéricas, sem o nível de identificação adequado;
- Outros problemas com as contas e políticas que possam contradizer/confrontar as diretrizes de direitos de acesso da BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA.

Comentado [FSdA1]: Como funciona esse processo ?

Controle de acesso à rede

- Quando o acesso remoto é necessário via VPN, uma solicitação deve ser feita a Dual Tech Informatica, passar por um fluxo de aprovação formal e seguir a política de redes segura;

- Terceiros ou visitantes que atuarem no escritório da BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA, devem passar por um processo formal de liberação da rede e os acessos devem ser controlados, pois para cada solicitação de acesso um registro das atividades deve ser mantido. Os acessos remotos também precisam ser levados em consideração no processo de desligamento, para que as contas sejam desativadas imediatamente. Verificar também os requisitos estabelecidos na política de BYOD;

POLÍTICA DE SENHAS

A senha na BORTONE ASSESSORIA CONTABIL E NEGOCIOS IMOBILIARIOS LTDA não deve ser compartilhada ou armazenada de qualquer forma. A senha é a forma mais convencional de identificação, deve ser um **recurso pessoal e intransferível,** que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

- Atenção: O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, devemos estabelecer os seguintes requisitos:

- A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesmo ser imediatamente alterada no caso de suspeita de sua divulgação;
- A senha inicial só será fornecida ao próprio colaborador, por meios seguros que assegurem a identidade do colaborador. Deve ser trocada no primeiro acesso;
- É proibido o compartilhamento de logins para funções de administração de sistemas;
- As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);
- Devem ser utilizadas ferramentas específicas para o armazenamento e gestão das senhas, como por exemplo um cofre de senhas;

As senhas deverão seguir os seguintes pré-requisitos:

Política de senha inclui os requisitos a abaixo:

- mínimo de tamanho: 8;
- máximo de tamanho: 64;
- Não permitir as últimas 32 senhas utilizadas;
- Pelo menos dever: 1 caractere maiúsculo, 1 caractere minúsculo, 1 símbolo e 1 número;
- Não permitir caracteres repetidos ou sequenciais;
- Não há expiração sem razão;
- Bloquear a conta após 5 tentativas incorretas de login;
- Deverá ser desbloqueada por procedimento interno e confirmação positiva;
- Não permitir o uso do nome e senhas comuns
- Não pode usar data de nascimento, nome da pessoa da família, cachorro, gato, número de RG ou CPF, números de telefone, placas de carros;

Para as senhas de administração, deve-se sempre trocar as senhas padrões fornecidas pelos sistemas/aplicações instalados e configurados. Para as senhas de administração deve ser considerado também:

- Senhas de administrador:
- ter um comprimento mínimo de 8 caracteres;
- ser formada por letras, números e caracteres especiais;
- não ser derivada de seus dados pessoais, tais como nomes de membros da família (incluindo animais de estimação), números de telefone, placas de carros, números de documentos e datas;
- não deve ser adivinhada por quem conhece a suas preferências pessoais (time para o qual torce, escritor, ator ou cantor favorito, nomes de livros, filmes, músicas etc.);
- Não estar presente em dicionários (de português ou de outros idiomas).

Da mesma forma, as senhas devem ser armazenadas de maneira segura nos bancos de dados e diretórios, incluindo *salt*. Os administradores de sistemas devem verificar a política de criptografia, para configurações técnicas.

Para fechar, o compromisso com o controle dos acessos

Para garantir o devido cuidado com os acessos, a segurança das informações, diversos fatores dependem da atenção dos colaboradores, precaução e o cumprimento dos processos.

Muitas violações de dados são causadas quando estas informações caem nas mãos de quem não deveria ter acesso. Portanto, deve ser verificado sempre se todos estão com os devidos acessos, somente os necessários e de acordo com os grupos, perfis e políticas de autorização, estabelecidas.

Pequenas ações que podem fazer uma grande diferença:

- Devemos manter a tela bloqueada quando nos ausentamos da estação de trabalho;
- Devemos manter a senha e as chaves de acesso de forma segura;
- Não devemos compartilhar em hipótese alguma os acessos com outras pessoas;
- Devemos certificar que estamos acessando as informações da empresa num local seguro e rede segura;
- Devemos separar as ferramentas do mundo profissional x pessoal;
- Devemos utilizar sempre senhas fortes!
- Não devemos registrar as senhas por escrito ou eletronicamente, em repositórios, notas, post-it, arquivos, e-mail ou outros.

Qualquer dúvida ou problema com o seu acesso entre em contato com o time de segurança da Dual Tech Informática.