DEPARTAMENTO DE INFORMÁTICA - TECNOLOGIA DA INFORMAÇÃO (TI)
1º REVISÃO DE MANUAIS DO PREVINIL 2° SEMESTRE DE 2022

REVISÃO

Esta revisão tem como objetivo acrescentar, reorganizar, anular e ou modificar procedimentos, normas, diretrizes e mapeamentos previamente citadas em manuais anteriores com o intuído de manter os procedimentos atualizados e em acordo com as leis vigentes, alem de ter fundamental importância nos aspectos de segurança da informação. Vale citar a observância da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados – LGPD e a norma ABNT NBR ISO/IEC 27001:2006 que versa sobre Sistema de Gestão de Segurança da Informação (SGSI).

Nos casos em que este documento anule ou modifique quaisquer procedimentos, normas, diretrizes e mapeamentos previamente publicados será explícito o documento e item onde se deu a alteração, sendo **citado o texto original** com formatação *itálica e cor vermelha* onde se deu a mudança, caso contrario as informações contidas neste documento devem ser consideradas complementos, apêndices e ou suplementos.

Todas as referencias a outras documentações do instituto serão realizadas utilizando-se da formatação ***negrito, itálico e sublinhado***.

INTRODUÇÃO

"Os dados são o aspecto mais importante do seu computador.
O hardware do computador pode falhar, os dados podem ser corrompidos, os computadores podem ser perdidos, roubados ou destruídos.
Você pode reinstalar sistemas operacionais e aplicativos, mas seus dados originais podem ser ***perdidos para sempre****."*

Massachusetts Institute of Technology – ***MIT***

Quando observamos pelo aspecto institucional os dados são de importância fundamental para o funcionamento dos tramites administrativos sua manutenção, segurança, integridade são fatores primordiais para o Departamento de informática (TI) do instituto.

Com a constante evolução e aprimoramento dos setores técnicos e tecnológicos do instituto se apresenta a necessidade de aprimoramento das documentações.

As informações apresentadas nesta documentação são necessárias para a manutenção de um ambiente seguro no nível técnico e operacional do setor de TI, refletindo assim em um ambiente seguro para todos os colaboradores do instituto.

1. CONTRODE DE ACESSO

1.1. USUARIOS E SENHAS - CONTROLE DE ACESSO LÓGICO

1.1.1. Cadastro Mapeamento/Manualização de procedimentos:

1.1.1.1 O cadastramento de usuários será realizado pelo departamento de TI do instituto sempre que provocado pelo presidente ou chefe de um dos departamentos do instituto, será respeitado a seguinte rotina:

1.1.1.2. O solicitante deverá fazer a solicitação ao departamento responsável;

1.1.1.3. O departamento responsável deverá verificar a necessidade de acesso do solicitante, recolher a documentação de cadastro do solicitante após a verificação documental encaminhar para o departamento de TI a solicitação;

1.1.1.4. O departamento de TI verificará a elegibilidade do solicitante junto com a política de segurança da informação, manuais e diretrizes do instituto;

1.1.1.5. O departamento de TI deverá determinar o tipo, nível, e autorizações de acesso e criar o usuário;

1.1.1.6. O departamento de TI deverá manter o acesso do novo usuário bloqueado até o solicitante assinar todos os termos de responsabilidade em vigência;

1.1.1.7. O departamento de TI liberará o usuário para acesso informando ao solicitante e ao departamento do solicitante.

1.1.1.8. Fluxograma:

*(*este fluxograma substitui o fluxograma de controle lógico posteriormente publicado* e pode ser melhor observado em documentação anexada publicamente no site do instituto seguindo o seguinte hiperlink: Tecnologia da Informação)

1.1.2. Níveis de usuário:

1.1.2.1. É responsabilidade do departamento de TI a atribuição de níveis de usuários no Active Diretory (AD) e em todos os sistemas utilizados pelo instituto.

1.1.2.2. Os níveis de usuários são utilizados para que cada usuário tenha acesso a apenas aplicações e informações que sejam de estritamente necessários para o desenvolvimento de sua função. Gerando assim uma camada adicional na Segurança da Informação.

1.1.2.3. As informações a respeito a acessos e liberações em cada nível de usuário é de responsabilidade do departamento de TI sendo estas informações classificadas como CONFIDENCIAL devendo este manter o controle de forma confidencial visando a manutenção da segurança da informação do instituto.

1.1.2.4. É responsabilidade do Chefe do departamento de TI e dos responsáveis pela gestão de acessos manterem o controle dos níveis de acesso.

1.1.2.5. Os responsáveis pela gestão de acessos serão designados pelo chefe do departamento de TI.

1.1.3. Senhas orientações gerais:

1.1.3.1. Alterações de Senha de usuário:

Uma das formas de diminuirmos a vulnerabilidade do fator humano dentro do setor de TI do instituto é aplicar uma política de mudanças de senha.

No entanto os usuários do nível administrativo e coorporativo não deverão alterar a senha sem prévia autorização, esta orientação não exclui a necessidade de troca de senha com periodicidade visando à manutenção de segurança na senha.

Antes da autorização de mudança de senha é importante observar se as credenciais não são utilizadas em outras aplicações, uma vez que caso as credenciais sejam utilizadas em outras aplicações estas serão interrompidas com a mudança, como podemos observar em exemplos práticos como:

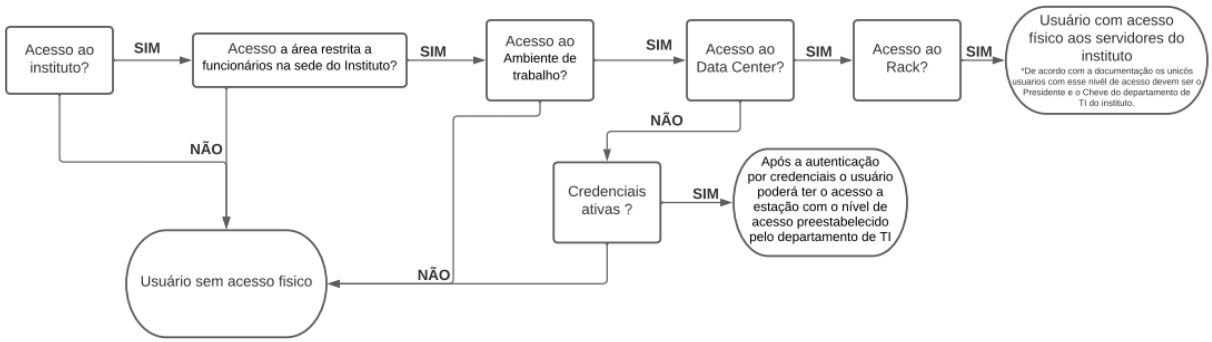
-E-mail corporativo que é utilizado em aplicações CLOUD como “DRIVE”;

-Credenciais utilizadas para autorização de aplicações como rotinas de backup ou autorização administrativa;

-Credencias com função de autorização dentro dos sistemas previdenciários;

1.2. UTILIZAÇÃO DA INFRAESTRUTURA DE TECNOLOGIA E ACESSO A INFORMAÇÕES - CONTROLE DE ACESSO FÍSICO

1.2.1. Complemento ao item ***6.6 do manual de informática, 2019, volume 1, edição 1,***;
Diagrama de controle de acesso físico Estações de trabalho / Ativos de informação / Servidores



*(Este diagrama e pode ser melhor observado em documentação anexada publicamente no site do instituto seguindo o seguinte hiperlink: Tecnologia da Informação)

1.2.1.1. Servidores de aplicações e dados:

O controle do acesso físico aos servidores de aplicações e dados do instituto se dá por diversas camadas de controle de acesso.

Os servidores se encontram dentro de Racks metálicos que são trancados com chaves, os únicos que possuem acesso as chaves dos Racks são o Presidente do instituto e o Chefe do departamento de TI.

Os Racks se encontram dentro de áreas com acesso controlado denominado Data Center que é um ambiente físico com controle de acesso realizado pelo departamento de TI.

O Data Center se encontra dentro a área restrita a funcionários na sede do Instituto.

O instituto se localiza em ambiente com controle de entrada e saída realizado por meio de funcionário e monitorado por câmeras de segurança;

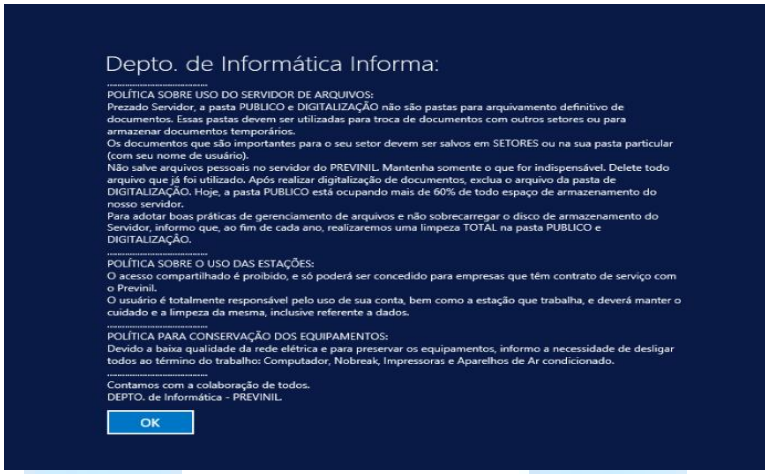
1.2.1.2. Ambiente de trabalho:
Todas as estações de trabalho conectadas a rede do instituto só podem ser acessadas através de autenticação de credenciais previamente cadastradas pelo departamento de TI;

1.2.2. Manual de Acesso Físico - Para o acesso de um usuário este deverá inserir suas credenciais de usuário e senha em qualquer dispositivo do ambiente de trabalho do instituto o dispositivo irá

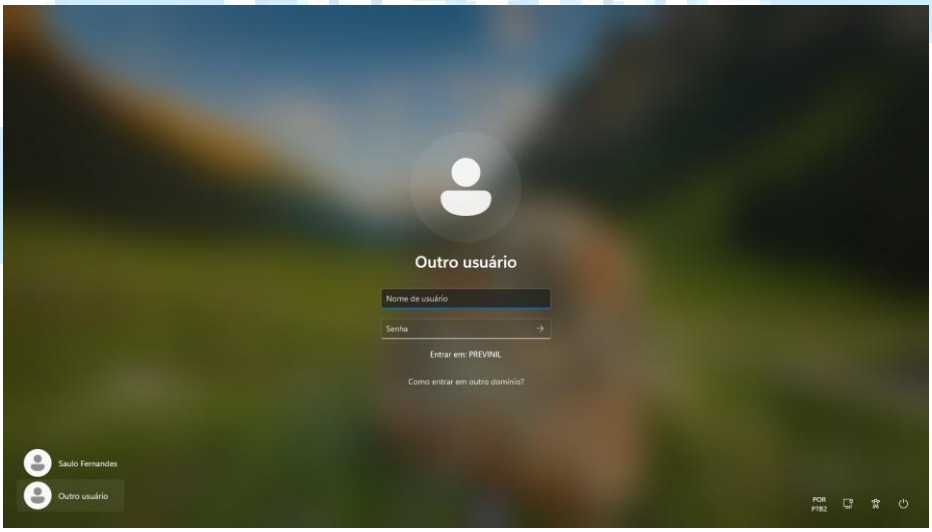
inicializar com todas as configurações previamente feitas por este usuário, como podemos observar no manual a seguir:

(1) O usuário autorizado a utilização de uma estação de trabalho deverá inicializar a estação, verificando se o Nobreak desta encontra-se ligado e acionando o botão “POWER” da estação;

(2) Após a inicialização do sistema o usuário deverá ler com atenção todas as diretrizes e informações contidas na tela inicial da estação de trabalho, após a leitura deverá clicar no botão “OK” como pode ser observado na imagem a baixo, seguindo assim para próxima etapa;



(3) Após o aceite das diretrizes e informações o usuário será direcionado para tela de LOGIN no sistema onde deverá utilizar suas credenciais para acessar a estação de trabalho;



(4) Após a autenticação do usuário ele poderá acessar as informações e programas previamente autorizados pelo departamento de TI;

2. CLASSIFICAÇÃO DE DADOS

Este item revoga o texto descrito no ***Manual de Informática 2019 Volume 1, Edição 1 e na Politica de segurança da informação – PREVINIL*** substituindo o item *6.5. CLASSIFICAÇÃO DA INFORMAÇÃO do Manual de Informática 2019 Volume 1, Edição 1 e* o item *6.5. CLASSIFICAÇÃO DA INFORMAÇÃO da Politica de segurança da informação – PREVINIL*, tendo à finalidade a atualização do texto em consideração a norma ABNT NBR ISO/IEC 27001:2006 que versa sobre Sistema de Gestão de Segurança da Informação (SGSI) e a LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados – LGPD.

Para darmos inicio a classificação de dados devemos considerar:

I - Dados – São valores atribuídos a algo. Registros soltos, aleatórios, sem qualquer análise ou estruturação.
II - informação - São dados, processados, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
III - documento - unidade de registro de informações, qualquer que seja o suporte ou formato;
IV - informação pessoal - Informação relacionada a pessoa natural identificada ou identificável;
V - informação pessoal sensível - informação pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
VI - Ativos de informação - São considerados ativos de informação os dados e/ou informações tratados ou não que fazem parte de sistemas de informações, podendo ser elas produzidas automaticamente pelo sistema, importadas de forma manual, importados de forma automática, ou seja, todos os dados e informações utilizados nos processamentos de sistemas informatizados, tendo como exemplos base de dados, banco de dados, backups. Assim como os meios de armazenamento, transmissão e processamento da informação.

2.1. **TIPOS DE CLASSIFICAÇÕES:**

2.1.1. Público: É uma informação do PREVINIL ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.
Não exige controle para acesso, distribuição, cópia ou devem ser públicos por força de Lei.

2.1.2. Restrito: Significa que é restrito ao PREVINIL, a um determinado setor, departamento ou destinatário não podendo ser retransmitida para fora da abrangência de restrição.
É uma informação que não se tem interesse em divulgar, onde o acesso por parte de indivíduos externos ao Instituto é proibido, devendo haver autorização caso necessário. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem do Órgão, porém, não com a mesma magnitude de uma informação confidencial.

O controle deve ser feito com acesso via autenticação de credenciais, quando não for possível, o acesso deverá ser controlado e mantido o registro de quando e quem teve o acesso à informação. Por sua natureza Informações pessoais e informações pessoais sensíveis sempre devem ser classificadas como restritas ou com uma classificação superior.

2.1.3. Sigiloso: Dados relativos à atividade empresarial de pessoas físicas ou jurídicas de direito privado obtidas por órgãos ou entidades distritais no exercício de atividade de controle, regulação e supervisão da atividade econômica cuja divulgação possa representar vantagem competitiva a outros agentes, Informações protegidas por alguma legislação de sigilo. Por exemplo: sigilo bancário, fiscal, comercial e segredo de justiça.
É uma informação crítica para os negócios do PREVINIL ou de seus Patrocinadores/Segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao PREVINIL ou aos seus Patrocinadores/Segurados.
Classificados como SIGILOSO nunca devem ser distribuídos, publicados, replicados. Seu controle deve ser realizado por verificação de credenciais preferencialmente deverá ser confeccionados em um documento único mitigando assim o risco quanto a segurança.

2.1.4. Confidencial: Deve ter o controle de acesso totalmente restrito a quem tem pela função desempenhada necessidade ao acesso. Dados, informações, documentos, ativos de informação com potencial risco de segurança para o instituto.
Ativos de informação devem impreterivelmente ser classificadas como confidencial.

REFERENCIAS

LEI N^{o} 8.159, DE 8 DE JANEIRO DE 1991.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados – LGPD

ABNT NBR ISO/IEC 27001:2006

Responsável pela elaboração do documento

Saulo Fernandes Dantas – Chefe do departamento de TI do PREVINIL

Nilópolis, 08 de julho de 2022