Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Acesso às Instalações Físicas.

Objetivo

Estabelecer regras para a gestão, controle e monitoramento do acesso físico às instalações da Instituição, especialmente nos locais em que há armazenamento ou fluxo de informações confidenciais ou sensíveis da Instituição.

Visão Geral

A gestão e o monitoramento do acesso físico às instalações são importantes para a segurança das informações mantidas pela Instituição, além de proteger a integridade física dos integrantes e dos demais ativos da Instituição.

1. Gerenciamento do Acesso Físico

Todas as instalações da Instituição devem ser fisicamente protegidas, observando-se à criticidade ou importância da função ou finalidade da área gerenciada.

O acesso físico a todas as instalações da Instituição deve ser registrado com câmeras de vigilância e através de controles físicos de acesso (biometria, interfone, porteiro).

O sistema de controle de acesso também deve abranger o acesso de visitantes externos da Instituição, através da identificação por crachás ou qualquer outro tipo de identificação que os segreguem dos demais integrantes da Instituição.

EMBRASI

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

O Responsável pela Segurança da Informação deve conceder credenciais de acesso aos integrantes da Instituição para que estes integrantes possam adentrar nas áreas restritas.

As credenciais de acesso serão periodicamente revisadas pelo Responsável pela Segurança da Informação. Também será realizado periodicamente um inventário completo dos ativos críticos da Instituição, incluindo características de onde estes ativos são mantidos e as medidas de controle de acesso aplicadas.

2. Gerenciamento de Credenciais de Acesso

A utilização de credenciais de acesso, tais como cartões ou chaves fornecidos pela Instituição, deve observar as seguintes diretrizes:

- As credenciais de acesso utilizadas pelos colaboradores não devem, em hipótese alguma, ser compartilhadas com outras pessoas;
- As credenciais de acesso não devem ter informações de identificação, salvo endereço de e-mail para retorno em caso de perda;
- As credenciais de acesso não mais necessárias devem ser revogadas pelo Responsável pela Segurança da Informação;
- O roubo ou extravio de credenciais de acesso será considerado um incidente de segurança da informação que deve ser informado de maneira imediata ao Responsável da Segurança da Informação.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

3. Gerenciamento de Acesso de Visitantes

O acesso de visitantes às instalações da Instituição deve observar as seguintes diretrizes:

- Os visitantes devem ser devidamente autorizados antes de adentrar nas dependências da Instituição, devendo ser escoltados em todos os momentos dentro de áreas de processamento e armazenamento de informações confidenciais.
- O acesso de visitantes deve ser rastreado através de registros de entrada e saída;
- O registro de atividades do visitante deve ser mantido para fins de auditoria, incluindo o seu acesso a quaisquer ativos informáticos onde eventuais informações confidenciais estejam sendo armazenadas ou transmitidas;
- O registro de visitantes deve documentar, no mínimo, o nome do visitante, seu registro de identidade, a empresa em que trabalha e o local, data e hora do acesso físico;
- O registro de visitantes deve ser mantido pelo tempo definido em Cronograma de Retenção elaborado pelo Responsável pela Segurança da Informação;
- Os visitantes devem ser identificados de maneira visível e distinta dos demais colaboradores da Instituição;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Os visitantes devem entregar o crachá ou identificação ao deixar a Instituição.

4. Gerenciamento de Acesso a Áreas Restritas

O acesso a áreas confidenciais nas dependências da Instituição deve observar as seguintes diretrizes:

- As áreas restritas da Instituição serão identificadas através da realização de inventário de ativos.
- Todas as áreas restritas devem possuir controle de acesso e todos os indivíduos presentes nessas áreas devem usar um crachá de identificação, de modo que tanto a imagem quanto as informações, no crachá, sejam ser claramente visíveis;
- Áreas restritas de armazenamento e processamento de informações, tais como *datacenters*, CPD, salas de computador, armários, roteadores de rede, salas de *hub*, salas do sistema de correio de voz e áreas similares que contenham recursos de tecnologia da informação serão restritas com base na necessidade funcional dos negócios realizados pela Instituição;
- Os ativos localizados em áreas não seguras devem ser protegidos através de medidas adicionais para preservar a integridade e a confidencialidade das informações confidenciais;
- Os dados armazenados pelas câmeras de circuito interno (CFTV), bem como dos demais mecanismos de controle de acesso devem ser mantidos pelo tempo

definido em Cronograma de Retenção elaborado pelo Responsável pela Segurança da Informação.

5. Gerenciamento de Acesso de Serviços Terceirizados

Os parceiros e prestadores de serviços terceirizados devem cumprir as leis e regulamentos aplicáveis sobre segurança contidos na Política de Terceirização da Instituição.

O Responsável pela Segurança da Informação designará um integrante da Instituição que seja confiável e tecnicamente experiente para acompanhar os funcionários de empresas terceirizadas que tenham que realizar atividades em áreas confidenciais.

No que tange ao acesso de funcionários terceirizados às áreas restritas da Instituição, devem ser observadas as seguintes diretrizes:

- Qualquer instalação ou desinstalação de software ou hardware será realizada pelo integrante de confiança designado;
- O funcionário terceirizado não deverá ter acesso visual ou eletrônico a quaisquer informações confidenciais ou restritas contidas no sistema por ele acessado;
- Dispositivos que exibem informações confidenciais em formulários de leitura humana devem ser posicionados de forma a evitar que o funcionário terceirizado leia essas informações de forma não autorizada;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- O funcionário terceirizado ao qual for concedido acesso desacompanhado à área física contendo informações confidenciais deve portar as credenciais de acesso adequadas.