Website

Unidade de Tecnologia de Informação
LINCE

Facebook

Gestão em Segurança da Informação na UNITI-LINCE

Servidor da
UNITI-LINCE
Carlos Machado

Diretor da
UNITI-LINCE
Everton W. Bocca

5 de agosto de 2020

Sumário

1 Introdução

O avanço científico tem conduzido rapidamente o armazenamento de dados da forma física à digital. As informações, anteriormente arquivadas sob o aspecto físico, essencialmente impresso, tranformaram-se, em razão do desenvolvimento tecnológico, em sistemas eletrônicos-digitais. O que era físico deixou de sê-lo, passando, gradativamente, do armazenamento óptico-magnético (CD/DVD) ao armazenamento digital.

Contudo, a evolução trouxe consigo aspecto inerente ao próprio armazenamento de dados e informação: sua proteção. Dito de outra forma, como proteger os dados armazenados de acessos indevidos e não autorizados? Há uma ampla, eficaz e correspondente modernização da segurança da informação capaz de conservar e preteger totalmente o conteúdo armazenado? A resposta é bem simples: não! Nenhum dado ou informação são completamente seguros e pensar de forma diversa beira à ingenuidade ou ao desconhecimento.

O que fazer então com a necessidade de armazenar e conservar conteúdos e informações? À semelhança do que acontece em outras searas tecnológicas, a segurança de dados também envoluiu e se antecipou aos possíveis danos, violações e acessos indevidos. O conceito de segurança, com isso, começou necessariamente a compreender a violabilidade, de modo que, a segurança se compõe também a partir da probabilidade de extinção e do risco de violabilidade. Sendo assim, a segurança é a redução do acesso indevido e a possível conservação do conteúdo, isto é, a gestão de risco em matéria de informação e dados.

Portanto, o dado, o conteúdo ou a informação, seja a armazenada, seja a transferida, jamais estarão completamente seguros e permanentemente convervados, mas através da gestão de riscos em segurança da informação é possível a redução significativa da vulnerabilidade e a máxima conservação dos dados catalogados. Há, para isso, dois parâmetros necessários em relação à segurança das informações ou dados: *(a) definir a segurança da informação (dado armazenado ou transferência); (b) planejar a gestão de riscos apropriada, considerando dinamicamente as interferências na segurança.*

O primeiro princípio *(a)* é excludente, ou seja, a segurança do dado em si ou sua transferência deve ser atendido separadamente, ainda que possuam ferramentas concomitantes (ex: criptografia ou uso de senhas). A definição sobre a pretensão de segurança -dado armazenado ou em transferência- é de suma importância e influenciará as demais camadas de gestão de risco e a modernização da segurança da informação. Enfim, *a gestão de segurança do dado armazenado, regra geral, é diferente do dado transmitido*.

Por sua vez, *(b)* planejar a gestão de risco, seja para o armazenamento ou transferência de dados, requer precisar o conceito de risco e o gerenciamento, considerando, nos dois casos, a aplicabilidade em um dado momento, local e equipamento. Em resumo, *risco* pode ser definido como potencial de eventos, contínuos ou isolados, capazes de gerar perdas. Por seu turno, *gerenciar riscos*, consiste em gerenciá-los, antecipar possíveis perdas e elaborar procedimentos que minimizem danos, considerando sua aplicabilidade em um certo equipamento ou equipamentos e em uma certa periodicidade.

2 Objetivos

2.1 Objetivos Gerais

- Definição do critério de segurança[1] *(dados armezados ou transferidos)*;
- Definição do sistema de segurança *(dados digitais ou dados físicos)*;
- Aplicabilidade da segurança *(Delimitação do período de gestão e do local de aplicabilidade)*;
- Gestão de risco *(prevenção)*[2];

2.2 Objetivos Específicos

- Segurança em relação aos dados armazenados *(segurança da informação)*;
- *Foco* na gestão de dados digitais;
- Gestão de segurança *permanente* e aplicabilidade na UNITI-LINCE;
- Planejamento e gestão do risco:

  I-Processo Ampliado *(conscientizar outras unidades e setores)*: As medidas de segurança da informação, aplicadas na Unidade, devem considerar, na medida do possível, interveniências externas. Nesta perspectiva, deve-se ampliar ao máximo a segurança e compartilhá-la com os agentes próximos da Unidade, como, por exemplo, outros setores do Centro Didático;

  II-Identificação dos riscos *(evento capaz de gerar dano)*: Identificar o risco consite: a-) entendimento; b-) mapeamento; c-) inspeção e d-) estudo;

  III-Análise de risco *(probabilibilidade de ocorrência, perda e violabilidade do conteúdo)*: a-) estimar a possibilidade de o evento ocorrer; b-) estimar o impacto e o dano;

  IV-Tratamento do risco: *(técnicas para lidar com o risco)* a-) desconsiderar o risco; b-) mitigar o risco;

  V-Implementação do controle: a-) orientação; b-) coordenação; c-)uniformização;

  VI-Avaliação e revisão dos riscos: a) acompanhamento; b-) monitoramento dos processos; c-) revisão contínua;

[1] Segurança da Informação se refere ao seu caráter estático, ou seja, o conteúdo ou dado armazenado. A segurança de informação compreende o dado armazenado, estático, e seu cartáter dinâmico, na concepção tranferência emissor/percurso/receptor e suas respectivas ferramentas.

[2] O gerenciamento de riscos compreende: (1) processo contínuo, (2) conduzido por todos os níveis organizacionais, (3) definição de estratégias, (4) identificação de potenciais riscos, (5) redução dos riscos e danos, (6) formação de procedimentos.

3 Gestão de Segurança da Informação na UNITI-LINCE

O planejamento e a implementação de gestão segurança considerou como objeto *(conteúdo carecedor de proteção)* toda e qualquer informação *(conteúdo digital ou físico)* recebida ou produzida no âmbito da Unidade. Assim, na UNITI-LINCE, todos os documentos administrativos, manuais, informações e dados, tiveram considerável tratamento de segurança, sejam os armazenados em domínio físico ou digital. Essa segurança, em especial a digital, desde sua implementação, considerou relevantes princípios da segurança da informação, a saber:

- Integralidade: *proteção contra modificação não autorizada*;
- Confidencialidade: *proteção contra o acesso indevido*;
- Disponibilidade: *disponibilização do conteúdo ou a informação, quando solicitados ou necessários*;

Também, observou-se o seguinte:

- Gestão em relação à segurança da informações armazenadas *(foco na gestão digital armanezada)*;
- Gestão em relação aos documentos oficiais e em relação aos produzidos na Unidade *(digitais ou digitalizados)*;
- Aplicabilidade em todos os computadores internos do setor e demais equipamentos administrados pela Unidade, como os das salas de aulas e os do *hall* do Centro de Educação;
- Ciclo de gestão de risco *(monitoramento constante)*;

3.1 Planejamento e gestão de risco em relação à segurança das informações digitais:

- I- Processo ampliado: O compartilhamento de ações em segurança da informação tem sido constantemente divulgados e incentivados pela Unidade. O *Relatório Anual 2019 UNTI-LINCE*, por exemplo, registrou a execução de diversas formatações em quipamentos administrados pela Unidade, visando:

  a) difusão do *Software Livre*;

  b) redução do risco de infecção por vírus;

  c) eliminação da vulnerabilidade da proteção por senhas;

  d) utilização de *sistemas operacionais livres ou licenciados*;

  e) realização de atualizações nos *sistemas operacionais livres ou licenciados*;

  Além disso, o relatório anual também apontou outras duas adversidades conexas às atualizações dos sistemas e resultante da conjunção *hardware/SO Windows* (e):

(e.1) desgaste espontâneo *(tempo de uso contínuo)*;

(e.2) limitação operacional *(adversidade na atualização)*;

Esses dois últimos desvios, (e.1) desgaste espontâneo e (e.2) limitação operacionacional, são destacados quando o *SO Windows* é instalado em equipamentos com elevado período de utilização e sobrevida. O desgaste espontâneo, causado pelo tempo de uso, tornam o equipamento obsoleto e, por isso, conduzem à dificuldade de atualização, limitação operacional e, em ultima análise, risco de segurança.

Por exemplo, a atualização do *Sistema Windows*, suas ferramentas de segurança e a própria versão, carregam, geralmente, vários pacotes, o que muitas vezes não podem ser renovados em equipamentos antigos, com tecnologia ultrapassada. Ademais, as licenças de utilização, quando disponibilizadas para equipamentos obsoletos ou superados, assimilam versões do *Sistema Operacionais Windows* antigas e sem suporte ou sem atualização dos recursos de proteção, causando, igualmente, risco à preservação dos dados e das informação.

- II-Identificação e análise dos riscos: Na gestão de segurança da informação digital, a Unidade identificou consideráveis vulnerabilidades:

  a) no *Sistema Operacional Windows*:

  1.problemas na atualização e correções de erros do sistema: *(ressalta-se: a atualização e a correção de erros são disponibilizadas pela empresa proprietária Microsoft)*. Em geral, entre o tempo de correção dos erros e a efetiva disponibilizaçao das atualização há um período de vulnerabilidade e incapacidade do *Sistema Windows (o sistema desatualizado não consegue carregar todos as ferramentas de segurança)*;

  2.incidência constante de vírus: no âmbito do Centro de Educação, a exemplo, está disseminado o vírus *"manoel.doc (.ex)"* que oculta conteúdos e altera registros, inclusive o do *Sistema Operacional Windows*;

  3.vulnerabilidade na proteção por senhas: por exemplo, o *Sistema Operacional Windows* permite, *in loco*, que usuário não autorizado acesse os dados armazenados no equipamento, mesmo sem possuir a senha de restrição (exemplo, há manuais disponiveis na internet que possibilitam, facilmente, o acesso e a alteração de senhas e *login* de usuários no *Sistema Operacional Windows)*;

  4.vulnerabilidade no compartilhamento de pastas no *Sistema Windows*;

  5.utilização de *softwares* não licenciados ou absoletos: causando, em geral, adversidades na atualização do *Sistema Windows (a falta de atualização, em especial das ferramentas de proteção, deixa o sistema vulnerável)*;

  6.utilização de versão não atualizada ou não licenciada do *Sistema Windows*: resultando, igualmente, prejuízos às ferramentas de proteção e, consequentemente, à segurança das informações e conteúdos armazenados;

  b) além das adversidades no *Sistema Windows*, obaservou-se que a utilização de ferramentas e procedimentos não institucionais geram insuficiência de controle

pelo usuário. Nesta forma, o controle de utilização e segurança são usualmente produzidos pela empresa que disponibilizou o serviço *(usuário depende **totalmente** da segurança produzida)*, cabendo ao usuário apenas utilizá-lo na forma e ferramentas concedidas *(exemplo: utilização de e-mail não oficial, ou disponibilização de conteúdos via Google Drive e não através do site institucional)*.

- III-Tratamento do risco: A Unidade, ao considerar os mecanismos e formas para enfrentar o risco de segurança, apreendeu os seguintes critérios:

  a) Considerar todo o conjunto de riscos e vulnerabilidades possíveis;

  b) Mitigar o risco é desenvolver mecanismos a níveis aceitáveis;

  c) Prevenir e reduzir o impacto e a probabilidade de perdas;

- IV-Implementação do controle e segurança da informação: A Unidade, visando implementar e gerenciar os mecanismos e os procedimentos de segurança em relação às informações e contéudos digitais, sob (a) orientação e (b) coordenação (*implementação das ferramentas somente após anuência do responsável pela Unidade)* e (c) uniformização *(procedimentos uniformes são mais fáceis de serem controlados)*, aplicou o seguinte:

  a) Instalação de *SO Livre Linux* em todos os equipamentos : Desde de 1999, a Unidade possui *Software Livre Linux* instalado nos equipamentos do setor e laboratórios e, atualmente, também nos equipamentos que administra, tais como, os computadores do *hall*, auditórios e salas de aulas do Centro de Educação. Cabe destacar, neste aspecto, que a Unidade também instala o *Sistema Linux* nos setores e salas de professores, quando solicitado pelo responsável e o equipamento seja bem público. Esse procedimento assegura:

  1.Autenticidade do Sistema Operacional Utilizado: A ultilização do *Sistema Operacional Linux* permite a aplicação de um Sistema Operacional licenciado e autêntico, afastando, assim, uso não autorizado e/ou não licenciado. Há que se compreender, ademais, que a utilização de sistemas não licenciados é sinonimo de risco de segurança, uma vez que *licença, atualização e ferramentas de segurança estão intimamente interligadas.*

  2.Autenticidade dos *Softwares* no *Sistema Operacional Linux*: A aplicação e disponibilização do *Sistema Operacional Linux*, além de permitir a utilização de um sistema autêntico e licenciado, também possibilita ao usuário dispor de um conjunto de *softwares* autênticos, licenciados e *"não piratas"*.

  3.Modernidade e Atualização do *Sistema Operacional Linux*: O *Sistema Linux*, ao disponibilizar atualizações períodicas e constantes, permite ao usuário utilizar um sistema moderno, genuíno e atual. A implementação desse controle de risco, por parte da UNITI-LINCE, viabiliza uma contínua e intensa preservação dos mecanismos e ferramentas de segurança do sistema utilizado na Unidade.

  4.Proteção Contra Vírus: A instalação do *Sistema Operacional Linux*, aplicada pela UNITI-LINCE como ferramenta de segurança, possibilita utilização de um

Sistema Operacional sem risco de vírus, preservando, nesta perpectiva, a integralidade e confidencialidade dos dados armazenados. Isto porque, em vista à vulnerabilidade do *Sistema Windows*, os vírus são construídos sob extensões *".exe ou .bat"*. Estas extensões são incapazes de serem executadas no *Sistema Linux*, revelando, nessa forma, um ambiente seguro e propício para armanezamento de dados.

5.Senhas e Usuários no *Sistema Operacional Linux*: Cumpre ressaltar que o *Sistema Linux* oportuniza criação de multiplos usuários e senhas *(o Sistema Operacional Linux oferece alta inviolabilidade de senhas)* diferentes ou iguais, conforme opção do usuário. No início da instalação, o *Sistema Linux* requer a criação de um usário e sua respectiva senha, conhecido, usualmente, como *"super usuário"*que gerenciará todas as atualizações e disposições do sistema. Além do *"super usuário"*, o *Sistema Linux* oferece também a criação de outros usuários, contudo, com algumas restrições e limitações, a depender das permissões conferidas pelo *"super usuário administrador"*. A UNITI-LINCE realiza esssa opção de segurança criando, a partir da instalação do *Linux*, dois usuários, um para utilização geral, com senha e *logins* divulgados para a equipe, e outro usuário administrador, com *login* e senha reservados e com divulgação restrita, onde serão armazenados os dados e conteúdos da Unidade. Além disso, para ampliar o parâmetro de segurança, os computadores administrativos contêm senhas e *logins* diferentes entre si e em relação aos demais equipamentos não administrativos, elevando, nesse sentido, o nível de segurança de informação na Unidade. Nesta oportunidade, convém destacar que a Unidade também emprega o *sistema dinâmico de senhas*, ou seja, a cada semestre, ano ou dependendo da necessidade *(exemplo: substituição de membro da equipe)* todas as senhas *(em especial as que permitem acesso à distância, como site ou dropbox)* são alteradas, a fim de reduzir eventuais riscos ao conteúdo armazenado. E, também, em razão ao *sistema dinâmico de senhas*, a UNITI-LINCE disponibiliza, aos equipamentos destinados à utilização geral da Comunidade do CE *(exemplo: os computadores instalados nas salas de aula ou no hall do CE possuem usuários e senhas de conhecimento geral)* senhas diferentes das empregadas na Unidade. Enfim, a aplicação do *sistema de senhas* e as proteções viabilizadas pelo *Sistema Operacional Linux* realizam elevados índices de gestão de riscos e de redução de perdas das informações.

6.Atualização e segurança de equipamentos obsoletos e antigos: O *Sistema Linux* permite o aproveitamento de equipamentos antigos e obsoletos, pois, além de ser um Sistema Operacional *leve*, plenamente adaptável em *hardwares* restritos e não modernos, viabiliza a contínua atualização de seu acervo de segurança.

b) Múltiplos dispositivos para armazenamento dos dados: Outro quesito de segurança da informação e dados digital utilizados pela UNITI-LINCE é o *sistema de múltiplo armanezamento*. Os dados e informações armazenados nos computadores administrativos são duplicados e copiados entre si e também armazenados em outros *hard disk* seguros, inclusive em disco rígido externo mantido em ambiente seguro e protegido.

c) Prioridade na utilização de ferramentas institucionais: A utilização de ferramentas e procedimentos institucionais permitem maior controle de segurança de dados, uma vez que, ao proporcionar estes serviços, a autarquia pública os desenvolve ou os adquire geralmente com todos os sistemas de proteção, segurança e suporte *(exemplo: atendimento ao usário)*. Neste aspecto, a UNITI-LINCE, priveligiando as ferramentas instutucionais, tem utilizado *site* e *e-mail* institucionais para agendamento de suas atividades ou disponibilização de seus conteúdos e notícias. As senhas de acesso a todos as ferramentas institucionais *(exemplo: e-mail ou site)* também são restritas a alguns membros da equipe e o acesso somente é permitido sob supervisão. Além disso, os dados inseridos nas agendas do *e-mail* ou no *site*, quando disponibilizados ao público, são destinados apenas à visualização, sem possibilidade de alterações ou exclusões de conteúdo ou informação gerada.

d) Autenticidade dos *softwares* e sistemas proprietários: A fim de garantir o direito intelectual de criação, a UNITI-LINCE não acrescenta ou instala Sistema Operacional ou *software* proprietário, privativo ou *não livre*, sem a respectiva lincença de utilização. A aplicação deste expediente garante não só o respeito às disposições legais relativos aos direitos autoriais, como também a utilização de um programa genuíno, *apto à atualizar suas ferramentas de segurança e proteção.*

- V- Reavaliação e revisão dos riscos:

  a) Atualização períodica do *Sistema Operacional Linux*: O *Sistema Operacional Linux*, ao disponibilizar atualizações constantes, permite intensa e periódica revisão dos mecanismos internos de segurança, o que compreende melhor resultado quanto à inviolabilidade e integralidade dos dados digitais armazenados. Diante disso, *a Unidade monitora e aplica constantemente as atualização em todos os computadores que possuem instalado o Sistema Operacional Linux*;

  b) Atualização do *Sistema Windows Licenciado*: A UNITI-LINCE também monitora e aplica, quando disponíveis, as atualização de segurança para o *Sistema Windows* instalado nos laboratórios, auditório do LINCE, Audimax e salas de aula do Centro de Educação. Essas atualizações, em geral, são essenciais para configurar proteção do sistema em tela e, consequentemente, assegurar a integralidade de todas as informações nele armazenadas.

  c)- Demais avaliações e revisões de risco no Sistema *Windows*: A Unidade, ampliando e avaliando seus mecanismos e procedimentos de gestão de segurança, tem revisado constantemente o *Sistema Windows*, a fim de identificar eventuais vírus ou programas maliciosos. Para isso, tem pesquisado e aplicado, permanentemente, alternativas para controlar ou reduzir a infecção desse sistema operacional:

  - **1.Instalação do Software Time Freeze** *(ferramenta de restauração)*: O *Software Time Freeze* (versão gratuita), instalado no SO *Windows* dos equipamentos dos laboratórios, auditórios e salas de aula do Centro de Educação, atua

como ferramenta de rastauração e, a cada nova execução do SO *Windows*, quaisquer alterações, armazenamentos ou instalações, inclusive de programas, são completamente excluídos do ambiente

- **2.Instalação e constante atualização do antivírus no SO *Windows*** *(procedimento indicado a todos que utilizam SO Windows):*
- **3.Configuração apropriada do antivírus para examinar todas extensões de arquivos** *(procedimento indicado a todos que utilizam SO Windows):*
- **4.Configuração apropriada do antivírus para examinar todas unidades de armazenamento** *(procedimento indicado a todos que utilizam SO Windows):*
- **5.Execução de somente um antivírus** *(procedimento indicado a todos que utilizam SO Windows):*
- **6.Utilização de programas originais e atualizados** *(procedimento indicado a todos que utilizam SO Windows):*
- **7.Criação de cópias de todo conteúdo em outras unidades de armazenamento** *(procedimento indicado a todos que utilizam SO Windows):*
- **8.Criação de ponto de restauração do sistema** *(procedimento indicado a todos que utilizam SO Windows):*

3.2 Planejamento e gestão de risco em relação à segurança das informações *não digitais*:

Além da gestão dos conteúdos e dados digitais *(armazenados)*, a UNITI-LINCE também realiza o tratamento das informações não digitais, vinculadas a diversos ambientes físicos. Incluem-se, nesta categoria, documentos oficiais, manuais, formulários, tutoriais e demais materias impressos, já que a gestão digital, em sua vez, compreendeu o meio no qual a informação eletrônica foi armazenada *(o armazenamento das mídias como CD, DVD, pendrive e HD externo foi tratada na gestão das informações digitais)*. Com base nisto, na gestão da informação *não digital* planejou-se:

- Cópia impressa dos principais documentos: A Unidade mantém cópia impressa e arquivada de todos os documentos oficias *(memorandos, ofícios, portarias, formulário etc...)* e dos principais tutorias e manuais produzidos pela equipe. Estes documentos são arquivados anualmente e, no prazo legal, são transferidos ao arquivo setorial do Centro de Educação. Entretanto, o último relatório UNITI-LINCE apontou a necessidade de revisão desse modelo de gestão, a fim de reduzir consideravelmente a utilização de papéis, impressos e folhas e de fomentar ainda mais a economicidade na Unidade. A alternativa mais propriada, ao que tudo indica, será substituição do consumo de papéis e impresso por modelos digitais ou plataformas institucionais *(exemplo: emissão e recebidmento de memorandos via portal RH; emissão de documentos via assinatura digital do portal RH; disponibilização de agendamentos via portal*

RH; termo de responsabilidade preenchido via portal RH; solicitação de informações e encaminhamos gerais via portal RH);

– Registro dos eventos também em agenda física: Atualmente, os eventos da Unidade *(reuniões, agendamentos dos ambientes e eventos em geral)* são também registrados em agenda física, para não inviablizar as atividades da Unidade, em caso de problemas na conexão de *internet* ou interrupção de energia elétrica. As mesmas considerações examinadas em relação ao consumo de papéis e folhas impressas, também cabe quanto ao registro das atividades do setor em agenda de papel: substituição completa por alternativas digitais e ou plataformas institucionais. Neste caso, a Unidade alinhar-se-á às alternativas e ferramentas disponibilizadas pela Autarquia Pública, cabendo a esta e não aos órgãos setorias, promover alternativas e opções para mantenção dos serviços públicos em caso de eventuais interrupções de conexão à *internet* ou suspensões de energia elétrica.

3.3 Difusão e demais ações de gestão das informações:

Por fim, cabe registrar que a Unidade também tem feito a gestão de certas circunstâncias e ações que possam refletir, ainda que indiretamente, nas informações e conteúdos emitidos, recebidos ou armazenados. São fatores que, de alguma forma, incidem na *integralidade, confidencialidade ou disponibilidade* da informação e, portanto, precisam ser conjugados. Neste contexo, o Plano de Prevenção Contra Incêndios, a publicidade de conteúdos nos *site* e a acessibilidade a informações e materias em computadores servidores, por exemplo, carecem ser planejados, analisados e revisados para que a informação seja preservada. Sendo assim, a UNITI-LINCE também sistematizou:

- I-Disponibilização de informações para a equipe: As informações para execução das atribuições da Unidade, quando necessárias para o conhecimento amplo e geral da equipe, são transmitidas diariamente pelo *e-mail* oficial. Contudo, visando agilidade na emissão, recepção e disponibilização dessas informações, a UNITI-LINCE mantém com todos os membros:

  a-) Grupo de *whatsApp e e-mail*;

  b-) Grupo de reuniões **preferencialmente** *online*, através de sistema de atividades ou de relatórios períodicos como, por exemplo, *Google Classroom ou Jitsi Meet*;

  c-) Permissão de acesso a materiais exclusivos no *site* da Unidade *(esse acesso é reservado à equipe UNITI-LINCE)*;

  d-) Permissão de acesso aos conteúdos disponibilizados no repositório digital de tutoriais e manuais *(esse acesso somente pode ser feito no Centro de Educação e somente membro da equipe pode fazê-lo)*;

  e-) Oficinas tecnológicas e de aprendizagem, destinadas à disseminação de informações, atualização e formação da equipe;

- II-Adequação ao PPCI: A Unidade considera o plano de prevenção contra incêncios essencial quesito, não só em relação à integridade das informações e dados produzidos no âmbiente público, mas, em especial, em relação à integridade da vida humana. Nesta perspectiva, a Unidade tem encaminhado períodicas solicitações de adequação do setor ao Plano de Prevenção Contra Incêndios disponível para a autarquia. Conforme constam no *Relatório Anual 2019 UNITI-LINCE.* e no *site* a Unidade, estas solicitações foram conduzidas desde 2016 às sucessivas gestões do Centro de Educação;

- Publicidade e a disponibilização de informações, conteúdos, materias: A Lei de Acesso à Informação, Lei nº 12.527/11, que regula o acesso à informação produzida ou acumuladas em órgãos públicos, dispõe que a regra é o acesso público. À vista disto, qualquer pessoa, ainda que não possua interesse direto, pode apresentar pedido de informações, bastando, para isso, simples identificação do conteúdo e dos dados pessoais. Em síntese, toda informação é publica e o sigilo, quando indicado, é uma exceção temporária, com prazo determinado e definido em lei. Como resultado dessas premissas, o aceso deve ser permitido por meio da transparencia ativa (disponibilização) ou transparencia passiva (providencialização). Há de se sublinhar: *a recusa ao acesso deve ser fundamentada pela administração através das regras de sigilo, catalogadas com antecedência para o dado ou conteúdo solicitado*. Diante de tais considerações, todos os documentos administrativos emitidos pela Unidade, são disponibilizados (transparência ativa) para acesso público no *site* da UNITI-LINCE, cumprindo, amplamente o principio da publicidade[3]. Além disso, os materiais - tutoriais, relatórios, manuais, publicações, informatívos - produzidos pela equipe somente são disponibilizados quando associados à lincença *creative commons* [4].

[3]Publicidade é condição de eficácia de todos os atos e documentos administrativos.

[4]Creative Commons é uma organização sem fins lucrativos que permite o compartilhamento e uso da criatividade e do conhecimento através de instrumentos jurídicos gratuitos.

4 Referências

CERT. Núcleo de Informação e Coordenação do Ponto BR. **Cartilha de Segurança para Internet**. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em 20 de junho de 2020.

BRASIL.Ministério da Educação. Universidade Federal de Santa Maria. Unidade de Tecnologia de Informação do CE - UNITI-LINCE-CE. **Relatório Anual de Ações Realizadas e Atendimentos**. Disponível em: <https://www.ufsm.br/laboratorios/lince/atendimentos/>. Acesso em 21 de janeiro de 2020.

BRASIL. Ministério da Educação. Universidade Federal de Santa Maria. Unidade de Tecnologia do CE - UNITI-LINCE. **Ata de Reunião Realizada no dia 7 de julho de 2020.** Disponível em: <https://www.ufsm.br/laboratorios/lince/wp-content/uploads/sites/762/2020/07/Ata-01-2020-Processo/23081023554202080.pdf>. Acessado em 08 de julho de 2020.

BRASIL. **LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 09 de junho de 2020.

BRASIL. **LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998.**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9609.ht>. Acesso em: 09 de junho de 2020.

HORI, Andre Shigueru. **Modelo de Gestão de Risco em Segurança da Informação: Um estudo de caso no mercado brasileiro de Cartões de Crédito.** Biblioteca Digital FGV, 2020. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle.pdf?sequence=2>. Acesso em: 20 de junho de 2020.

CREATIVE COMMONS. **O que é Creative Commons?**. Disponível em: <https://br.creativecommons.org/sobre/>. Acesso em: 20 de junho de 2020.

BRASIL. Fundação Escola Nacional de Administração Pública. **Classificação de Informações e Dados Abertos**. Disponível em: <https://repositorio.enap.gov.br/bitstream/Classificação/Informações.pdf>. Acesso em 27 de junho de 2020.

Correa, Instituto Sardezo. Escola Superior do Tribunal de Contas da União. **Mundo Conectado**. 2020. Brasilia.

Correa, Instituto Sardezo. Escola Superior do Tribunal de Contas da União. **Controle da Administração**. 2020. Brasilia

BRASIL. Ministério da Educação. Universidade Federal de Santa Maria. Unidade de Tecnologia de Informação do CE - UNITI-LINCE-CE. **Relatório Anual de Ações Realizadas e Atendimentos**. Disponível em: <https://www.ufsm.br/laboratorios/lince/atendimentos>. Acesso em 18 de março de 2020.

BRASIL.Fundação Escola Nacional de Administração Pública. Cursos e Eventos. **Acesso à Informação no Brasil**. Disponível em: <https://enap.gov.br/pt/cursos>. Acesso em 27 de junho de 2020.