1.OBJETIVO

Este procedimento tem como objetivo definir regras para assegurar a segurança da informação, garantido a sua confidencialidade, integridade e disponibilidade.

2.MODO DE PROCEDER

2.1 Autenticidade

A autenticidade é a garantia de que a identidade da entidade com a qual se está a comunicar corresponde àquela desejada. Em outras palavras, a autenticidade reside no fato de as duas partes de uma comunicação terem a certeza de que estão a trocar informações com a entidade correta.

A autenticidade tem como função garantir que no decorrer de uma comunicação, as entidades são quem dizem ser, o que permite garantir a origem da informação. Pode ser garantida através de:

- Assinatura Digital (as assinaturas digitais em utilização, pelos Utilizadores do ISEP, foram geradas por uma entidade externa ao ISEP, sendo da responsabilidade desses utilizadores efetuar a sua gestão);
- Certificado Digital: os certificados digitais destinam-se a autenticar um servidor perante um utilizador. São requeridos pela Secção de Infraestruturas e Suporte ao Utilizador à FCCN para todos os servidores com acesso HTTPS e FQDN distintos.

A Assinatura digital é um método de autenticação da informação digital, tipicamente análoga à assinatura física em papel. A utilização de uma assinatura digital garante que uma mensagem veio do emissor fidedigno. Para verificar este requisito, a assinatura deve ter as seguintes propriedades:

- Autenticidade – permite que ao recetor confirmar que a assinatura foi feita pelo emissor;
- Integridade – permite garantir que a mensagem não foi modificada (qualquer alteração, fará com que a assinatura não seja válida);
- Não repúdio – garante que o emissor não possa negar a autenticidade da mensagem.

2.2 Confidencialidade

A confidencialidade é a propriedade que limita o acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

De modo a limitar o acesso à informação aos utilizadores autorizados, é limitada através de: Passwords e Controlo de Acesso.

2.2.1 Passwords

Todas as passwords definidas deverão respeitar as seguintes condições:

- Ter um comprimento mínimo de 9 caracteres e máximo de 16;

- Não conter o nome de utilizador;
- Cumprir 3 dos seguintes 4 requisitos: carateres maiúsculos, minúsculos, numéricos, 1 carater do seguinte grupo [! @ H * - _ + , . ?].

As passwords ficam registadas no sistema de acessos do sistema de autenticação do IPP.

2.2.2 Controlo de Acesso

Considerando que a autenticação assegura a legitimidade do acesso, é necessário que os novos utilizadores tenham definido as suas permissões de acesso, quer às aplicações, quer à rede.

2.2.2.1 Aplicações/rede

- Docentes, Trabalhadores Não Docentes, Bolseiros e Investigadores

Sempre que um novo Docente, Trabalhador Não Docente, Bolseiro ou Investigador seja admitido, a Divisão de Recursos Humanos (DRH), atribui um Utilizador comunicando por helpdesk@isep.ipp.pt à Secção de Infraestruturas e Suporte ao Utilizador (SISU). Mediante o perfil do novo Trabalhador, é associado um nível de autorização para os seguintes recursos informáticos:

- Rede;
- Portal;
- Webmail;
- Moodle.

Caso o recurso humano tenha necessidade de acesso aos recursos informáticos administrativos, com autenticação autónoma, é necessário obter a aprovação do Diretor de Serviço/Chefe de Divisão (dono da aplicação) ou a aprovação da Presidência.

A SISU é responsável por atribuir a palavra-chave. O Trabalhador deverá deslocar-se à SISU para proceder ao levantamento da palavra-chave.

- Estudantes

As credenciais são criadas automaticamente pelos Serviços de Sistemas Informáticos (SSI) de acordo com as listas de ingresso ou listas homologadas de candidatos admitidos. As credenciais criadas contem uma Palavra-chave temporária e são transmitidas por SMS. No primeiro acesso ao sistema o estudante é obrigado a modificar a sua Palavra-chave.

2.3 Integridade

A integridade é a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

A proteção da informação contra modificação, sem a permissão explícita do proprietário daquela informação, é garantida através de Antivírus.

É da responsabilidade do utilizador, realizar periodicamente a verificação da existência de vírus no PC, recorrendo à aplicação antivírus instalada e existente para o efeito. Na eventualidade da existência de vírus que não possam ser removidos com essa aplicação, o utilizador deverá efetuar um pedido de suporte à SISU, efetuando um pedido através do portal do ISEP.

No caso dos servidores, é da responsabilidade da SISU, efetuar verificações periódicas de existência de vírus.

2.4 Disponibilidade

A disponibilidade é a propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Para assegurar ao utilizador, o acesso aos dados sempre que necessário, estão definidas um conjunto de medidas de contingência e de recuperação.

2.4.1 UPS e gerador

Os servidores primários estão ligados a duas unidades de alimentação ininterrupta (UPS) e a um gerador de emergência, com capacidade de 24 horas.

2.4.2 Backup´s

A segurança da informação é garantida através de um sistema de backup descrito na Instrução de Trabalho, Backup's (SSI-SISU-IT001).

2.4.3 Plano de contingência e recuperação

Em situações de desastre, a SISU deve proceder às seguintes ações:

- Detetar e determinar uma condição de desastre;
- Notificar as pessoas responsáveis para recuperação;
- Informar os Diretores de Serviço/Chefes de Divisão;
- Prover serviços de ajuda à recuperação – contactar, se necessário, empresas fornecedoras de equipamento que possam ajudar à recuperação.

2.4.3.1 Plano de Contingência

2.4.3.1.1 Falha de disco de sistema físico

Deverá proceder-se da seguinte forma:

- Trocar o disco danificado e formatá-lo;

- Instalar o sistema operativo;
- Instalar o *software* de base;
- Efetuar procedimento de reposição da informação (ponto 2.4.3.2).

2.4.3.1.2 Falha de sistema virtual

Deverá proceder-se da seguinte forma:

- Avaliar a falha;
- Repor imagem do sistema, caso aplicável, ou:
    - Instalar o sistema operativo;
    - Instalar o *software* de base;
- Efetuar procedimento de reposição da informação (ponto 2.4.3.2).

2.4.3.1.3 Avaria grave

Após a disponibilização de servidor ou espaço no servidor procede-se do seguinte modo:

- Instalar a Base de Dados a partir do último *backup*;
- Proceder à reposição do sistema na SISU.

2.4.3.1.4 Falha de ar condicionado

A temperatura de inlet nos servidores não deve ser superior a 25°C, sendo esta monitorizado por sistema específico de monitorização ambiental do centro de dados.

No caso de uma falha do ar condicionado, esta deve ser considerada uma avaria de grande prioridade, sendo de imediato comunicada à entidade responsável pelo contrato de manutenção específico do centro de dados e seus subsistemas ou Secção de Manutenção (SMT), caso não exista contrato de manutenção específico.

2.4.3.1.5 Falha de energia elétrica

No caso de falha de energia elétrica, dever-se-á notificar a Secção de Manutenção e acompanhar a situação de modo a tomar as medidas necessárias

No caso da falha de energia elétrica se relacionar com falha nos subsistemas do centro de dados, como por exemplo, unidades de alimentação ininterrupta (UPS), quadro inversor, diferenciais/disjuntores, ou outros, dever-se-á notificar também a empresa responsável pelo contrato de manutenção do centro de dados e seus subsistemas de modo a tomar as medidas necessárias

Se a energia não se restabelecer ao fim de 20 horas, e não for possível garantir a operação com recurso ao gerador de emergência, dar-se-á início ao desligar controlado dos sistemas.

2.4.3.1.6 Alarme de incêndio

Em caso de disparo do sistema de deteção de incêndios do centro de dados, deverá proceder-se:

- Averiguar da gravidade da situação;
- Desligar todos os equipamentos ou a energia, caso o evento não esteja controlado por via do sistema de deteção e extinção automática de incêndio, existente no centro de dados.
- Contactar os serviços correspondentes – portaria ou segurança.

2.4.3.1.7 Inundações ou infiltrações

O centro de dados dispõe de um sistema de monitorização específico que permite a deteção automática de inundações ou infiltrações no seu interior:

Neste caso proceder do seguinte modo:

- Averiguar da gravidade da situação, nomeadamente se o evento ocorre no interior ou exterior do centro de dados e se afeta diretamente o mesmo;
- Caso a gravidade do mesmo demonstre essa necessidade, proceder ao desligar controlado dos sistemas;
- Contactar a SMT, caso se trate de um evento no exterior do centro de dados ou a empresa responsável pelo contrato de manutenção do centro de dados caso o evento esteja diretamente relacionado com os subsistemas que o compõem.

2.4.3.2 Plano de recuperação

Sempre que, face a uma falha, haja necessidade de repor a informação perdida, o procedimento é o seguinte:

- Repor o último backup, ou imagem do sistema;
- Estabelecer as ligações a Bases de Dados, caso necessário;
- Atualização dos dados a partir do último backup, através dos documentos de alterações com data posterior ao último backup.

2.5 Controlo dos Registos

Os registos são arquivados de acordo com o descrito no procedimento, Gestão documental (UAG-GPQ-PG001).

3.APROVAÇÃO

Aprovado por: Serviços de Sistemas Informáticos (Nuno Silva) _____