




UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

POLÍTICA DE SEGURIDADE DA INFORMACIÓN


Código: POSI-001

Data de aprobación: 14 de febreiro de 2011

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>2 de 10</b> |

## CONTROL DO DOCUMENTO

| Referencia  | Nome do Documento                     |                                | Clasificación      |
|---|---------------------------------------|--------------------------------|--------------------|
| POSI-001  | Política de Seguridade da Información |                                | Público            |
| Versión   | Data                                  | Propósito/descrición do cambio | Data Revisión      |
| 1.0   | 18/01/11                              | Aprobación                     | N/A                |
|   |                                       |                                |                    |
| Autor   |                                       | Aprobado por                   | Data de aprobación |
| Área TIC. Unidade de Seguridade.  |                                       | Consello de Goberno            | 14/02/11           |
| <b>Distribución</b>   |                                       |                                |                    |
| Este documento atópase dispoñible ó público na web da Universidade de Santiago de Compostela.   |                                       |                                |                    |
| <b>Control de versións</b>  |                                       |                                |                    |
| O Responsable de Seguridade da Área TIC é o responsable do control de versións deste documento.   |                                       |                                |                    |
| <b>Control de Calidade</b>  |                                       |                                |                    |
| O Comité de Seguridade da Información é responsable da revisión do Documento, no marco do seguimento periódico da Política de Seguridade da Información, ou como consecuencia de cambios significativos, e en coordinación coas auditorías de seguridade. |                                       |                                |                    |

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>3 de 10</b> |

## ÍNDICE

|    |                                    |    |
|----|------------------------------------|----|
| 1. | INTRODUCCIÓN .....                 | 4  |
| 2. | OBXECTIVOS .....                   | 4  |
| 3. | ALCANCE.....                       | 6  |
| 4. | PRINCIPIOS XERAIS .....            | 6  |
| 5. | ORGANIZACIÓN DE SEGURIDADE.....    | 8  |
| 6. | APROBACIÓN E ENTRADA EN VIGOR..... | 10 |

|  |  |                            |                           |
|--|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|  |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>4 de 10</b> |

## 1. INTRODUCCIÓN

A información é un activo estratéxico para a Universidade de Santiago de Compostela (USC), e debe ser axeitadamente protexida, sexa cal sexa a forma na que estea representada, almacenada ou sexa procesada.


Neste entorno compre destacar o papel das Tecnoloxías da Información e das Comunicaci3ns (TIC) pola crecente importancia no tratamento desa informaci3n, sendo o rápido desenvolvemento destas tecnoloxías un dos factores principais que está a permitir que as Administracións Públicas melloren a súa eficiencia, posibilitando achegarse ó cidadán mediante novas canles de comunicaci3n. Pero a informaci3n e as tecnoloxías que a tratan están sometidas a riscos, internos e externos, que é necesario xestionar adecuadamente para situalos baixo limiares aceptables.

Neste eido a USC propoñe utilizar sistemas de xestión e normas que permitan xestionar adecuadamente a seguridade da mesma, coma poden ser a norma ISO/IEC 27001:2005, "*Information technology - Security techniques - Information security management systems - Requirements*", ou o Esquema Nacional de Seguridade, no eido da administración electrónica.

Compre ter presente que a seguridade da informaci3n precisa da colaboraci3n e implicaci3n de toda a comunidade universitaria, dende os 3rganos directivos, que aproban a presente política e son responsables da súa divulgaci3n e implantaci3n efectiva, ata os usuarios finais dos sistemas de informaci3n. Por iso, toda a organizaci3n debe estar preparada para previr, detectar, reaccionar e recuperarse ante posibles incidentes de seguridade.

## 2. OBXECTIVOS

A Universidade de Santiago de Compostela define a presente Política de Seguridade da Información, de carácter **obligatorio** para toda a comunidade universitaria e empresas colaboradoras, tendo coma obxectivo fundamental garantir a seguridade da informaci3n e a prestaci3n continuada dos servizos que proporciona, actuando preventivamente,

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>5 de 10</b> |


supervisando a actividade e reaccionando con presteza fronte ós incidentes que poidan ocorrer.

Esta Política debe sentar as bases para que o acceso, uso, custodia e salvagarda dos activos de información, dos que se serve a USC para desenvolver as súas funcións, se realicen baixo garantías de seguridade, nas súas distintas dimensións:

- **Integridade:** propiedade ou característica consistente en que o activo de información non sexa alterado de xeito non autorizado.
- **Dispoñibilidade:** propiedade ou característica dos activos consistente en que as entidades ou procesos autorizados teñan acceso ós mesmos cando o requiran.
- **Confidencialidade:** propiedade ou característica consistente en que a información nin se poña a disposición, nin se revele a individuos, entidades ou procesos non autorizados.
- **Trazabilidade:** propiedade ou característica consistente en que as actuacións dunha entidade poidan ser imputadas exclusivamente a dita entidade.
- **Autenticidade:** propiedade ou característica consistente en que unha entidade sexa quen di ser ou ben que garanta a fonte da que proceden os datos.

Baixo estas premisas os obxectivos específicos da Seguridade da Información na USC serán:

- Velar pola seguridade da información, nas distintas dimensións antes descritas.
- Xestionar formalmente a seguridade, en base a procesos de análise de riscos.
- Elaborar, manter e probar os plans de continxencias e continuidade da actividade que se definan para os distintos servizos ofrecidos pola USC.
- Realizar unha adecuada xestión de incidencias que afecten á seguridade da información.
- Manter informado a todo o persoal acerca dos requirimentos de seguridade, e difundir boas prácticas no manexo da información.
- Proporcionar os niveis de seguridade acordados con terceiras partes cando se compartan ou cedan activos de información.

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>6 de 10</b> |

- Cumprir coa regulamentación e normativa vixente.

Está Política de Seguridade:

- Aprobárase formalmente polo Consello de Goberno.
- Revisarase regularmente de xeito que se adapte as novas circunstancias, técnicas ou organizativas, e evite a obsolescencia.
- Comunicarase a todos os empregados e ás empresas externas que traballen coa USC.


### 3. ALCANCE

A Política de Seguridade aplícase a toda a comunidade universitaria e ós seus activos de información: ó seu persoal e alumnos; á información xerada, procesada e almacenada, independentemente do seu soporte e formato, utilizada en tarefas operativas ou administrativas; á información cedida dentro dun marco legal establecido, que será considerada como propia a efectos exclusivos da súa protección; a tódolos sistemas utilizados para administrar e xestionar a información, sexan propios da USC ou alugados ou licenciados pola mesma. Esta Política afecta tamén as empresas colaboradoras.

### 4. PRINCIPIOS XERAIS


Os principios xerais da Política de Seguridade da Información da USC son:

- A seguridade enténdese coma un proceso integral constituído por todos os elementos que posibilitan un sistema de información: técnicos, humanos, materiais e organizativos.

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>7 de 10</b> |

- A USC desenvolverá a súa Política de Seguridade no marco da Lexislación vixente relativa a protección de datos de carácter persoal, propiedade intelectual, e calquera outra lexislación autonómica, estatal e europea de aplicación.
- A análise de riscos será a base para determinar as medidas de seguridade que se deberán implantar. Esta análise manterase permanentemente actualizada dentro dun ciclo de mellora continua.
- A xestión da seguridade da USC buscará a redución dos custes a través dunha xestión optimizada da seguridade da información.
- Evitaranse os riscos derivados dunha falta de segregación de funcións.
- O acceso ós sistemas de información realizarase, salvo naqueles casos nos que non sexa posible, a través de credenciais persoais e intransferibles.
- O nivel de acceso ós sistemas de información estará baseado nas necesidades do posto de traballo do usuario, aplicando o principio de mínimo privilexio.
- Os equipos informáticos e o software empregaranse para fins estritamente relacionados coas funcións da USC e nunca para fins persoais ou distintos dos aprobados.
- A seguridade dos sistemas de información debe contemplar os aspectos de prevención, detección e corrección para conseguir que as ameazas sobre os mesmos non se materialicen ou non causen danos graves.
- Todos os usuarios dos sistemas de información son responsables da comprensión e cumprimento da Política de Seguridade e das normas, procedementos, instrucións e recomendacións asociadas.
- Desenvolveranse a concienciación, capacitación e educación en materia de seguridade da información.
- Deberá designarse un propietario para cada activo de información. Esta, ademais, clasificarase en función da confidencialidade da mesma.

Os principios xerais, anteriormente descritos, serán adecuadamente desenvolvidos mediante normativa específica.

|   |  |                            |                           |
|---|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>8 de 10</b> |

## 5. ORGANIZACIÓN DE SEGURIDADE

A fin de garantir a correcta implantación da presente Política a USC organizarase co obxecto de definir as medidas de seguridade que deberán aplicarse ós activos de información, e que deberán ser implantadas pola Área TIC.

Dita organización da seguridade contará coa participación activa da alta dirección da USC, quen aprobará a Política de Seguridade da Información e asignará e/ou delegará responsabilidades nas persoas que considere axeitadas, e periodicamente será informada para asegurar o seguimento da implantación efectiva da mesma.

Igualmente, a organización implicará en distinta medida a todo o persoal da USC, co obxecto de estender a implantación das prácticas de seguridade axeitadas.

Dentro da organización a definir crearase un **Comité de Seguridade**, que estará composto por representantes dos seguintes órganos unipersoais ou áreas:

- O Reitor, ou persoa na que delegue.
- Xerencia.
- Secretaría Xeral.
- O Director da Área TIC.
- O Responsable de Seguridade da Área TIC.

Cada órgano unipersoal, vicerreitoría, servizo e áreas designarán os seus representantes e suplentes, para substituílo en caso de ausencia. Está designación farase constar no documento POSI-003-Membros do Comité de Seguridade.

Asemade, unha vez constituído, o comité poderá propoñer a incorporación ao mesmo de ata dous PDI, pertencentes a departamentos ou áreas de coñecementos relacionados coa seguridade nos sistemas de información, co obxecto de que aporten a súa experiencia e coñecementos ao comité tanto no eido tecnolóxico coma no eido legal.


|  |  |                            |                           |
|--|--|----------------------------|---------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>      |
|  |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>9 de 10</b> |

As **funcións do Comité de Seguridade** serán as seguintes:

- Promover a integración dos requisitos de seguridade cos obxectivos estratéxicos da USC.
- Asegurarse de que a Política de Seguridade teña en conta o marco legal vixente, incluíndo o referido a protección de datos de carácter persoal, propiedade intelectual.
- Coordinar a implantación da Política de Seguridade.
- Revisar a efectividade da Política de Seguridade e mantela actualiza.
- Definir as pautas xerais en materia de Seguridade da Información a través da normativa desenvolvida.
- Publicar e difundir a normativa relativa á seguridade da información entre todos os afectados.
- Revisar os informes de incidencias de seguridade máis significativas.
- Controlar as ameazas sobre a información e outros activos.
- Investigar e actuar para previr incidencias de seguridade.
- Definir roles e responsabilidades das distintas funcións relacionadas coa seguridade da información.
- Promover o desenvolvemento de iniciativas destinadas á melloras da seguridade.
- Definir as accións a seguir no caso de situacións non previstas, en relación á seguridade da información ou ante casos de incumprimento da normativa.
- Manter informado ao equipo de alta dirección da USC das iniciativas relevantes en materia de seguridade promovidas na USC.

Ademais de formar parte do comité de seguridade, o Responsable de Seguridade da Área TIC terá as seguintes funcións e responsabilidades específicas:

- Asegurar a definición de metodoloxías e procesos de seguridade homoxéneos en toda a USC.

|   |  |                            |                            |
|---|--|----------------------------|----------------------------|
|  | <b>POLITICA: Política de<br/>Seguridade da Información</b> | <b>CÓDIGO<br/>POSI-001</b> | <b>VERSIÓN<br/>1</b>       |
|   |  | <b>DATA<br/>14/02/2011</b> | <b>PÁXINA<br/>10 de 10</b> |

- Controlar as incidencias de seguridade e coordinar as accións correctoras pertinentes.
- Colaborar co resto do persoal técnico no desenvolvemento das iniciativas de seguridade.
- Asesorar ás distintas unidades técnicas na definición e implantación de procedementos e de medidas técnicas.
- Promover na USC as medidas de concienciación necesarias en materia de seguridade da información.

## **6. APROBACIÓN E ENTRADA EN VIGOR**

Esta Política de Seguridade da Información apróbase o día 14 de febreiro de 2010, polo Consello de Goberno, entrando en vigor nesa data, tendo validez ata a súa substitución por unha nova Política.