**POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN**

| **Elaborado por:** | **Revisado por:** | **Aprobado por:** |
| --- | --- | --- |
| Juan Iturbe A.  09/01/2019 |  |  |

1. **INTRODUCCIÓN**

La presente política nace desde la necesidad de identificar los activos de información de la Unidad X de la Organización Y (ORG\_Y) y definir las responsabilidades de protección adecuadas para cada uno de ellos. Una vez identificados los activos de información se podrán clasificar de acuerdo a su valor, sensibilidad, confidencialidad, integridad y disponibilidad requeridas por la ORG\_Y. Una vez clasificados los activos de información, se podrán proponer e implementar controles adecuados al nivel de seguridad requerido para cada clasificación.

La presente política se encuentra alineada con los objetivos estratégicos “Mejorar la calidad, cantidad y gestión de los recursos” y “Consolidar la cultura de excelencia en todos los procesos de la ORG\_Y”. En el caso del primer objetivo, al mejorar la calidad y gestión de uno de los activos más importantes de la ORG\_Y, la información. En el segundo caso, al desarrollar mecanismos de control y gestión de los activos de información dentro de los procesos académicos y administrativos de la ORG\_Y.

1. **OBJETIVO**

Establecer las bases de un sistema de clasificación de la información, con el fin de proteger la confidencialidad, integridad y disponibilidad de la misma. La información se clasificará para señalar su necesidad, prioridad y el grado de protección que ésta requiere, tomando en cuenta su valor, requerimientos legales y normativos e importancia para la ORG\_Y.

1. **ALCANCES**

La presente política es aplicable a toda la información que sea de propiedad y/o en custodia del Decanato.

1. **DOCUMENTOS RELACIONADOS**

Los documentos relacionados con la presente política se listan a continuación:

* Leyes y normativa externa
  + Ley 19.223 (1993): Ley de delitos informáticos.
  + Ley 19.496 (1997): Protección de los derechos del consumidor.
  + Ley 19.628 (1999): Ley de protección de la vida privada.
  + Ley 20.285 (2008): Sobre acceso a la información pública.
  + Ley 17.336 (2012): Ley de propiedad intelectual.
  + Ley 21.091 (2018): Sobre educación superior.
  + Regulación europea para la protección de datos (GDPR - General Data Protection Regulation, 2018).
  + Política Nacional de Ciberseguridad (2017).
  + ISO/IEC 27000:2014: Sistemas de gestión de la seguridad de la información (SGSI), Visión de conjunto y vocabulario.
  + ISO/IEC 27001:2013: Sistemas de gestión de la seguridad de la información (SGSI), Requisitos.
  + ISO/IEC 27002:2017: Código de prácticas para los controles de seguridad de la información.
* Normativa interna
  + Reglamento general de régimen de estudios de pregrado (2011).
  + Reglamento de convalidaciones de asignatura de Pregrado (2002).
  + Reglamento de traslados (2011).
  + Reglamento de movilidad estudiantil internacional USACH (2012).
  + Reglamento general de los programas de Magíster Académicos (2015)
  + Reglamento general de los programas de Magíster Profesional (2015)
  + Reglamento general de régimen de estudio de pregrado (2011)
  + Reglamento complementario de régimen de estudios de la ORG\_Y (2012)
  + Fija normas para la eliminación de documentos de los archivos de la universidad (1980)
  + Modifica y complementa la resolución N°3.269 (1999)

1. **DEFINICIONES**

La presente política se desarrolló en base a lo establecido en la ISO/IEC 27002:2017 sobre “Clasificación de la información”, por lo que en ésta se aplican las definiciones allí incluidas y las indicadas en la ISO/IEC 27000. De todas formas, para mayor claridad, las siguientes definiciones se basan en ésta norma y la legislación vigente sobre protección de datos personales:

* *Activo:* Es todo recurso que tenga valor para la ORG\_Y. La ORG\_Y tiene diferentes tipos de activos: activos relacionados con el entorno (edificios, instalaciones, equipamiento) y personal, activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones), activos relacionados con la información (datos, documentos impresos y digitales), activos relacionados con las funciones de la ORG\_Y (productos, servicios) y activos intangibles (credibilidad, conocimiento acumulado).
* *Confidencialidad:* Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
* *Control:* Medida que modifica un riesgo.
* *Custodio de la información*: Es cualquier persona que mantiene bajo su responsabilidad información de la cual no es propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo a la importancia de los activos .
* *Propietario de la información*: Es el responsable de que su información se encuentra inventariada, clasificada y se protege debidamente. Además es el responsable de definir y revisar periódicamente las restricciones de acceso y clasificación de activos de información importantes. Finalmente se preocupa del manejo adecuado para el borrado o destrucción de sus activos de información.
* *Datos de carácter personal o datos personales*: los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
* *Datos sensibles*: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
* *Disponibilidad:* Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.
* *Integridad:* Propiedad de exactitud y completitud.
* *Política:* Intenciones y dirección de una organización, de acuerdo a cómo las expresa formalmente su alta dirección.
* *Riesgo:* Probabilidad de ocurrencia de un evento indeseado que puede traer consecuencias negativas.

1. **RESPONSABILIDADES**

* *Comité de Seguridad de la información:* Comité de alto nivel que responde ante el Decano de la ORG\_Y y que busca mantener un nivel de seguridad acorde a las necesidades de la ORG\_Y y sus recursos disponibles.
* *Encargado de la Seguridad de la Información (ESI) u Oficial de Seguridad de la Información (OSI):* Es el representante del Decano en la definición y aplicación de los criterios de seguridad de la información en la ORG\_Y, es responsable de supervisar el fiel cumplimiento de las políticas de seguridad, su normas, procedimientos y estándares.
* *Propietario de la información*: Es el responsable de que su información se encuentra inventariada, clasificada y se protege debidamente. Además es el responsable de definir y revisar periódicamente las restricciones de acceso y clasificación de activos de información importantes. Finalmente se preocupa del manejo adecuado para el borrado o destrucción de sus activos de información.
* *Custodio de la Información*: Supervisa e implementa mecanismos que garanticen la protección de la información, según las definiciones realizadas por los propietarios de dicha información.
* *Funcionarios de la ORG\_Y y unidades dependientes:* Tienen la responsabilidad de cumplir con lo establecido en el presente documento y aplicarlo tanto en su entorno laboral, como fuera del mismo. Además, tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

1. **POLÍTICA**

Las siguientes declaraciones componen la política de clasificación de información:

* 1. La información y los activos de información son recursos críticos y de alto valor estratégico para la ORG\_Y, por lo tanto deben ser protegidos y resguardados.
  2. Los propietarios de los activos de información serán los responsables de su clasificación.
  3. La clasificación de la información será actualizada anualmente o cuando ésta se modifique.
  4. Se establecerá un procedimiento de clasificación de la información transversal a la ORG\_Y. Esta incluye al menos:
     1. Identificación de los activos de información.
     2. Una evaluación de riesgo para cada activo de información a clasificar, incluyendo a los activos, tecnologías y procesos que lo soportan.
     3. La participación directa del propietario y custodio del activo de información.
  5. La información es clasificada de acuerdo a los siguientes criterios de valoración, tomando en cuenta su importancia y se protege de acuerdo a esta clasificación.
     1. *Confidencial:* Es toda aquella información que de ser revelada sin autorización o manejada por entes no autorizados, puede causar graves daños a la Unidad X. El uso de este tipo de información requerirá de previa autorización por parte del Propietario de la información y la suscripción de acuerdos de confidencialidad para mayor protección. Esta clasificación incluye por ejemplo a) La información privada o personal de los estudiantes, funcionarios y académicos b) Información referente al ámbito privado de los usuarios; c) Resultados de las evaluaciones de desempeño de los funcionarios y académicos; y d) Cualquier otra información que la Universidad, la ORG\_Y y/o la ley establezcan como confidencial. Su revelación tiene un impacto serio sobre los objetivos estratégicos a largo plazo o pone en riesgo la supervivencia de la ORG\_Y.
     2. *Restringido:* Para aquella información que puede ser revelada solamente a cierto grupo de personas. Su revelación puede tener un impacto significativo a corto plazo sobre las operaciones y objetivos estratégicos de la ORG\_Y. El uso de este tipo de información puede requiere de previa autorización por parte del Propietario de la información y posiblemente la suscripción de acuerdos de confidencialidad para mayor protección.
     3. *Uso Interno:* Es aquella información que es única y exclusivamente para uso interno de la ORG\_Y. Esta información incluye toda aquella información que requiere de cierto nivel de protección pero que no cumple con los criterios necesarios para ser clasificada como Confidencial. Ejemplos no restrictivos de este tipo de información lo constituyen: a) Algunas Políticas, Estándares, Procesos, Procedimientos, Lineamientos y otros comunicados formales de la ORG\_Y, aplicables únicamente a la misma; b) Reportes de las distintas áreas; c) Memorandos y/o ordinarios; d) Directorios internos, entre otros. La revelación de esta información puede causar incomodidad menor o molestias operativas menores.
     4. *Información Pública:* Es toda aquella información que se genera para su divulgación pública. Para esta información sólo se deben de implementar los controles adecuados para asegurar la integridad y disponibilidad de la misma. Su revelación no conlleva daños.
  6. Inventario de activos de información: Se deben identificar y clasificar los activos de información, su naturaleza (digital o física), descripción de su contenido, idioma, formato del soporte, locación, tiempo de vida, propietario y custodio de la información. Para ello, se registrará dicha información en un documento a cargo del encargado de Seguridad de la información, que tendrá el mismo tratamiento de un activo de información. Serán los propietarios de la información registrados, quienes deben informar formalmente al encargado ante cualquier cambio que se produzca sobre su activo de información y que afecte al presente registro.
  7. Identificación de activos que soportan el ciclo de vida de la información: En base al registro anterior, se deben identificar los activos relevantes para el ciclo de vida de los activos de información y documentar su importancia. El ciclo de vida de la información incluye su creación, tratamiento, almacenamiento, transmisión, borrado y destrucción. Cada activo identificado debe tener asignado un propietario. Estos también se deben inventariar en un documento a cargo del encargado de seguridad de la información. Los activos identificados deben tener el mismo nivel de protección que el activo de información que soportan.
  8. Eliminación de los activos de información: Anualmente se procederá a la ejecución de un procedimiento de eliminación de los activos de información (de acuerdo a su formato) que hayan cumplido su tiempo de vida. Se debe prestar especial atención, en aquella información que pueda tener un valor histórico para la Universidad o el país, en cuyo caso se debe revisar la posibilidad de su traslado con el archivo patrimonial de la Universidad.
  9. Etiquetado de la información: Se establecerá un procedimiento de etiquetado de la información transversal a la ORG\_Y. Esta debe incluir al menos:
     1. Los activos de información tipo documento digital o físico deben contener una etiqueta ubicada en la parte superior derecha de la primera página en donde se indique su clasificación. El formato de las etiquetas será la misma para todos los documentos.
     2. Para el etiquetado de activos de información procesados sobre sistemas de información se debe incluir la clasificación en sus metadatos.
     3. Para documentos clasificados como públicos, no es necesario dicho etiquetado.

1. **DIFUSIÓN**

La presente política, sus normas, procedimientos y estándares, y sus actualizaciones y/o modificaciones se publicarán en la web de la ORG\_Y. El encargado de seguridad de la información será el responsable de gestionar la publicación correspondiente.

1. **REEVALUACIÓN**

La presente política, sus normas, procedimientos y estándares serán examinados y reevaluados por el Comité de Seguridad de la información cada un año y extraordinariamente cuando ocurra un incidente de seguridad que afecte a un activo de información con riesgo medio y/o alto, de manera de introducir las modificaciones apropiadas.

1. **CUMPLIMIENTO**

El cumplimiento de las políticas de seguridad, sus normas, procedimientos y estándares, deberá ser una tarea cotidiana y de estricta aplicación por parte de la comunidad de la ORG\_Y. El incumplimiento de la presente política expone a quien la vulnere a las sanciones pertinentes según sea el caso.

1. **CONTROL DE VERSIONES DEL DOCUMENTO**

| **Versión** | **Fecha** | **Creador** | **Revisor** | **Aprobador** | **Notas de la versión** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 08/01/2019 | Juan Iturbe |  |  | Versión final 1.0 |
| 1.1 | 10/01/2019 | Juan Iturbe |  |  | Inclusión de responsabilidades custodio y propietario de la información. |
| 1.2 | 11/12/2019 | Juan Iturbe |  |  | Revisión del documento, inclusión de atributos en el inventario de activos de información. |
| 1.3 | 28/05/2020 | Juan Iturbe |  |  | Actualización sobre la eliminación de activos de información e inclusión del tiempo de vida de los activos. |