Universidad Icesi

JUNTA DIRECTIVA
Resolución No. 52
(10 de agosto de 2016)

"Por la cual se aprueba el documento de la Política de Seguridad de la Información de la Universidad Icesi"

La Junta Directiva de la Universidad Icesi, en uso de sus atribuciones estatutarias,

RESUELVE:

ARTÍCULO PRIMERO.- Aprobar la Política de Seguridad de la Información de la Universidad Icesi que fue presentada a su consideración en la reunión del 3 de agosto de 2016.

ARTÍCULO SEGUNDO.- El documento de Política de Seguridad de la Información queda como se escribe a continuación:

Universidad Icesi

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Universidad Icesi está comprometida con la protección de la información crítica asociada con los procesos de enseñanza – aprendizaje y de investigación, y con las actividades administrativas propias de la institución. De igual manera, la Universidad está comprometida con la protección de la información de los diferentes grupos de interés: estudiantes, profesores, colaboradores y público en general. En concordancia con este compromiso, la Universidad reconoce la importancia de la seguridad de la información y de los sistemas que apoyan todas las actividades de la Universidad.

ARTÍCULO 1º.- PRINCIPIOS

Con el fin de dar cumplimiento a la misión, visión, valores centrales y objetivos institucionales, la Universidad Icesi ha establecido los siguientes principios fundamentales que soportan la política de seguridad de la información:

Por ser la información uno de los activos más valiosos e importantes de la Universidad Icesi, se debe:

a) *Promover su uso responsable y ético.*
b) *Mantener la confidencialidad de la información de acuerdo a su clasificación, independientemente del medio o formato donde se encuentre.*
c) *Preservar su integridad, sin importar la forma en que sea transmitida o su permanencia y/o temporalidad.*
d) *Asegurar su disponibilidad para los casos en que sea requerida.*

ARTÍCULO 2º.- LINEAMIENTOS GENERALES

La Universidad Icesi define y aprueba las siguientes directrices generales, con el objetivo de orientar las acciones relacionadas con la seguridad de la información, para lograr los objetivos institucionales.

a) *La información debe ser protegida*

La información es un activo vital de la Universidad y por lo tanto debe ser protegida por todos.

b) *La información debe contar con un responsable*

Toda la información utilizada por la Universidad para el desarrollo de sus actividades debe tener asignado uno o más responsables, quienes tomarán las decisiones que sean requeridas para su protección y determinarán los privilegios de uso. Así mismo, todas las personas que integran la comunidad universitaria son responsables de la seguridad de la información que reciben por parte de la institución.

De igual manera, la seguridad de la información personal es responsabilidad de cada integrante de la comunidad universitaria.

c) *La información debe ser clasificada*

Los responsables de la información deben clasificarla basados en su valor, sensibilidad, riesgo de pérdida y/o requerimientos legales de retención.

d) *El manejo de la información debe cumplir con las regulaciones legales*

La comunidad universitaria se compromete a cumplir con la regulación nacional e internacional de seguridad de la información.

e) *La propiedad intelectual de la información se debe preservar*

Mientras se tenga una relación contractual o como estudiante, la propiedad intelectual sobre investigaciones realizadas, libros o revistas escritas, patentes o derechos de

autor, será propiedad de la Universidad, de acuerdo al reglamento de propiedad intelectual de la Universidad Icesi.

f) ***La seguridad de Información deberá ser parte de la gestión de los sistemas de información de la Universidad***
Los requerimientos de seguridad de la información deben ser identificados: (a) antes del diseño de los nuevos sistemas de información; (b) durante los ajustes de los sistemas actuales o; (c) durante los cambios tecnológicos que se requieran, de tal manera que se asegure el cumplimiento de la política de seguridad de la información.

g) ***Se debe asegurar la autenticidad de la información generada por la Universidad***
Se deberá asegurar la autenticidad de las comunicaciones electrónicas internas y externas que realice la Universidad.

h) ***La seguridad de la información será de conocimiento imperativo para la comunidad universitaria***
Es obligación de la comunidad universitaria, sin excepción alguna, conocer, respetar y cumplir las políticas de seguridad de la información de la Universidad, desde su ingreso hasta su retiro.

i) ***Debe existir capacitación continua y creación de cultura en seguridad de la información***
La Universidad dispondrá de un programa permanente de creación y consolidación de la cultura de la seguridad de la información. En estos programas deben participar los colaboradores, profesores, estudiantes y terceros.

j) ***La comunidad universitaria debe comprometerse a usar adecuadamente los servicios y recursos de información.***
Los servicios y recursos de información de la Universidad son únicamente para propósitos de la institución y deben ser usados como activos para la realización del trabajo requerido.

k) ***La identificación y autenticación a cualquier activo será personal***
El acceso a cualquier información o activo de información de la Universidad debe estar controlado mediante una autenticación personal.

l) ***Debe existir un control y una administración del acceso a la Información***
Se deben establecer mecanismos de control de acceso físico y lógico para prevenir accesos no autorizados a los activos que almacenan la información de la Universidad.

La información confidencial de la institución debe mantenerse con acceso restringido cuando no es utilizada. La comunidad universitaria debe respetar esos controles.

m) ***Debe existir un plan de administración de incidentes***
Se contará con un programa de manejo de incidentes que permita gestionar y resolver las situaciones o acciones que violen la política de seguridad.

n) ***Debe existir una gestión del riesgo en seguridad de la información***
Los riesgos a que está expuesta la información y los activos de información de la Universidad, deben ser identificados, evaluados y mitigados de acuerdo a su valor, probabilidad de ocurrencia e impacto.

o) ***Debe existir un plan de continuidad del negocio para la Universidad***
Todos los activos de información y los procesos asociados a los objetivos institucionales deben contar con un plan de continuidad, un plan de recuperación de desastres, y estar preparados para ataques contra la seguridad de la información.

p) ***Deben existir mecanismos de seguridad para los servicios de red de la Universidad***
Se debe asegurar la confidencialidad, integridad y disponibilidad de la información trasmitida sobre la red institucional de la Universidad.

q) ***Los terceros que utilizan y/o accedan, local y remotamente a los activos de información de la Universidad están obligados a cumplir con la política de seguridad de la información***
El uso o acceso por parte de terceros a los activos de información de la Universidad que sean clasificados como confidenciales, debe ser formalizado por medio de acuerdos que hagan obligatorio el cumplimiento de la política de seguridad de la información.

ARTÍCULO TERCERO.- **La** presente resolución rige a partir de la fecha de su expedición.

Se firma en Santiago de Cali, a los diez días del mes de agosto del año dos mil dieciséis.

FRANCISCO JOSÉ BARBERI OSPINA
Presidente

MARÍA CRISTINA NAVIA KLEMPERER
Secretaria General