Pontificia Universidad JAVERIANA Cali

DIRECTRIZ 01 /16
VICERRECTORÍA ADMINISTRATIVA CALI
(Directriz Sobre la Seguridad de la Información en la Seccional)

El Vicerrector Administrativo de la Pontificia Universidad Javeriana Seccional Cali

CONSIDERANDO:

1. Que la Pontificia Universidad Javeriana Cali (PUJ Cali) considera la información como un activo esencial para sus actividades y en consecuencia necesita protección adecuada, dado que puede estar expuesta a una variedad de amenazas y vulnerabilidades.

2. Que teniendo en cuenta el incremento de los riesgos asociados a la información, la Javeriana Cali se compromete a asegurarla y con este fin decide implementar el Sistema de Gestión de Seguridad de la Información (SGSI).

3. Que la Javeriana Cali creó la Coordinación de Seguridad de la Información adscrita al Centro de Servicios Informáticos, en adelante la Oficina de Seguridad de la Información (OSI), quien será la encargada de establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el SGSI siguiendo los lineamientos de la norma ISO 27.000, o la que la actualice o sustituya.

4. Que en desarrollo del artículo 79 de los Estatutos y del 139 y siguientes del Reglamento Orgánico de la Seccional, se expide la presente Directriz.

RESUELVE:

ARTÍCULO PRIMERO. - Expedir la siguiente Directriz sobre el manejo y tratamiento de la Seguridad de la Información en la Seccional:

DIRECTRIZ SOBRE LA SEGURIDAD DE LA INFORMACIÓN

1. Alcance.

La presente Directriz cubre a todas las actividades de la PUJ Cali. Por lo tanto, éstas deben ser diseñadas teniendo en cuenta los lineamientos dados por el SGSI, los cuales se encuentran descritos en este documento y en el documento de *"Normas Institucionales para el uso de tecnologías de información"*.

Todo usuario de la información, sean estos estudiantes, docentes, colaboradores, terceros, egresados y/o visitantes, está obligado a seguir los lineamientos de esta directriz y de las normas y procedimientos que se derivan de ella. Los incumplimientos a las mismas se considerarán como violaciones a la confianza entre la PUJ Cali y el usuario, y por tanto estos son susceptibles a acciones disciplinarias conforme a la magnitud y característica del aspecto no cumplido según las normas establecidas.

2. Objetivo.

El objetivo de esta directriz es asegurar la confidencialidad, integridad y disponibilidad de la información. Se definen estos atributos según la norma ISO27001:

a) ***Integridad***: se refiere a la propiedad de salvaguardar la exactitud y completitud de los activos de información[1]. Para la PUJ Cali es importante esta propiedad puesto que mantener la información íntegra le permite una adecuada toma de decisiones y un registro fiable de las transacciones de la Universidad.

b) ***Confidencialidad:*** se refiere a la propiedad que determina que la información no sea revelada a individuos, entidades o procesos no autorizados[2]. Para la PUJ Cali es importante esta propiedad, puesto que le permite asegurar que la información de estudiantes y en general de la comunidad universitaria que poseemos permanezca reservada y accesible solo a personal autorizado.

c) ***Disponibilidad:*** se refiere a la propiedad de la información que asegura que esta esté accesible y pueda ser usada bajo demanda por una entidad autorizada[3]. Para la PUJ Cali esta propiedad es importante puesto que le permite una operación efectiva y eficiente al asegurar que la información se pueda acceder en el momento oportuno.

3. Roles y responsabilidades.

La Vicerrectoría tiene a su cargo la gestión general sobre la seguridad de la información en la PUJ Cali, incluyendo los niveles de acceso asignados a cualquier persona y con las tecnologías de información en general.

Atendiendo al compromiso con la seguridad de la información, la Vicerrectoría define los siguientes roles (y sus atribuciones) que actúan en el Sistema de Gestión de la Seguridad de la Información (SGSI) para dar cumplimiento a esta directriz:

---

1 NTC-ISO/IEC 27001. Tecnología de la Información TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LAINFORMACIÓN (SGSI). REQUISITOS. 2011. Pág. 3

2 NTC-ISO/IEC 27001. Tecnología de la Información TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LAINFORMACIÓN (SGSI). REQUISITOS. 2011. Pág. 2

3 NTC-ISO/IEC 27001. Tecnología de la Información TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LAINFORMACIÓN (SGSI). REQUISITOS. 2011. Pág. 3

3.1. El Vicerrector.

Tiene como responsabilidades:

a) Definir la directriz, actualizaciones y sus mejoras a partir de las sugerencias originadas por el grupo asesor de seguridad de la información.
b) Definir cambios en el alcance del SGSI a partir de las sugerencias emitidas por el grupo asesor.
c) Definir los lineamientos por los cuales se rige el SGSI.
d) Aprobar el documento de normas institucionales para el uso de tecnologías de información y comunicación.

3.2. El Grupo Asesor de Seguridad de la Información (GASI).

Está compuesto por el Vicerrector Administrativo, Director del Centro de Servicios Informáticos y el Coordinador de Seguridad de la Información. Tiene como función principal asesorar al Vicerrector Administrativo en el gobierno del SGSI. Por lo anterior tiene a su cargo:

a) Sugerir al Vicerrector Administrativo cambios en el alcance del SGSI, es decir, qué procesos se deben incluir.
b) Verificar el avance en el control de riesgos y su efectividad en los procesos ya incluidos en el SGSI.
c) Estudiar y sugerir las mejoras al SGSI propuestas por la OSI.

3.3. La Oficina de Seguridad de la Información (OSI).

Es la encargada de la implementación y mejora continua del SGSI siguiendo las directrices de la Vicerrectoría Administrativa. Adicionalmente tendrá a su cargo las siguientes actividades:

a) Planear, implementar, verificar y mejorar el SGSI.
b) Proponer al GASI las mejoras a la directriz de Seguridad de la Información.
c) Sugerir al GASI los cambios en el alcance del SGSI.
d) Determinar una metodología de evaluación de riesgos.
e) Levantar el inventario de activos de información asociados a los procesos incluidos en el alcance.
f) Identificar las amenazas, vulnerabilidades e impactos asociados a los procesos. Construir mapa de riesgos.
g) Seleccionar, sugerir, implementar y/o monitorear controles frente a los riesgos,
h) Definir los responsables de activos de la información y de las tecnologías que la soportan (sistemas de información, equipos de cómputo, documentos, etc.), conocidos en conjunto como activos de información.
i) Ejecutar la asignación de roles a personas según las orientaciones de los responsables de los activos de Información (mirar el punto 4.5) y
j) Sugerir las normas institucionales para el uso de tecnologías de información y comunicación.
k) Evaluar y coordinar la implementación de los controles de seguridad de la información.
l) Realizar auditorías periódicas para establecer las acciones de mejora que contribuyan a fortalecer los hallazgos identificados.

3.4. Responsables de Activos de información (RAI).

Se denominarán "Responsables de Activos de Información", todas las personas, que, por su condición, relación o cargo con la Universidad, deban manejar o tengan acceso a cualquier información perteneciente a la PUJ CALI. Los Responsables de Activos de Información tendrán a su cargo las siguientes responsabilidades:

a) Determinar los roles que se deben utilizar para la ejecución de funciones sobre los activos de información.
b) Definir las funciones asignadas a cada rol.
c) Autorizar la asignación de roles a las personas adecuadas.
d) Verificar una adecuada segregación de funciones.
e) Asegurar la eliminación de roles a personas, cuando estos ya no son requeridos.
f) Verificar periódicamente la integridad y coherencia de los activos de información producto de los procesos de su área.
g) Hacer cumplir las normas y directrices expedidas por la OSI por las personas autorizadas de su área.
h) Reportar a la OSI los hallazgos en cuanto a situaciones que afecten la seguridad de la información de los activos a su cargo.
i) Seguir los lineamientos que le sean asignados por la OSI y
j) Responder por las violaciones a la seguridad de información de los activos a su cargo.

3.5. Usuarios de Información.

Son "Usuarios de Información" todas las personas que usan los activos de información de la PUJ CALI. Estos usuarios tendrán a su cargo las siguientes responsabilidades:

a) Cumplir la Directriz y las normas de seguridad de la información expedidas por la Vicerrectoría Administrativa.
b) Reportar cualquier incidente de seguridad que afecten los principios de la seguridad de la información y
c) Responder por violaciones a la seguridad de información originadas por el incorrecto uso de sus permisos.

4. Revisión y aprobación.

De manera general la Directriz de seguridad de la información, sus normas complementarias y los procedimientos, serán revisados por la OSI cada tres (3) años, o cuando sea requerido por cambios legales o sustanciales en la infraestructura o activos de información de la PUJ CALI. Los cambios serán aprobados por el Vicerrector Administrativo.

5. Documentos de referencia.

a) Norma ISO/IEC 27001, capítulos 5.2 y 5.3
b) Norma NTC-ISO/IEC 27001. Tecnología de la Información TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LAINFORMACIÓN (SGSI). REQUISITOS

c) Metodología de evaluación y tratamiento de riesgos
d) Normas y directrices institucionales para la Seguridad de Información

6. Terminología básica sobre Seguridad de la Información.

- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad puede estar involucradas. [ISO/IEC-27002-2007]

- **Sistema de gestión de seguridad de la información**: conjunto de procesos que se encargan de planificar, implementar, mantener, revisar y mejorar la seguridad de la información. [NTC-ISO/IEC-27002-2007]

- **Activos**: cualquier cosa que tenga valor para la organización. [NTC 5411-1-2006]

(Hasta aquí el texto de la Directriz)

ARTÍCULO SEGUNDO. Vigencia y derogatorias. La presente Directriz entrará en vigencia a partir de la fecha de su expedición, y deroga todas las disposiciones que le sean contrarias.

Dado en Cali, 1 de noviembre de 2016.

PONTIFICIA UNIVERSIDAD JAVERIANA
Vicerrectoría Administrativa

Carlos Rodrigo Montehermoso Jaramillo
Vicerrector Administrativo de la Seccional