CONSEJO PROFESIONAL NACIONAL DE ARQUITECTURA Y SUS PROFESIONES AUXILIARES

POLÍTICA RELACIONES CON PROVEEDORES

Código	PA-GC-11
Versión	1
Tipo	Politica
Implementación	13/09/2017
Alcance	
Nivel de confidencialidad	

1. OBJETO

Preservar los niveles de seguridad y privacidad de los activos de información de la Entidad que sean accedidos o administrados por proveedores, a través de la implementación de controles que minimicen los riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad de la información.

2. ALCANCE

Aplica a todos los trabajadores y terceros que accedan y operen activos de información de la Entidad

3. DEFINICIONES

CONFIDENCIALIDAD
DISPONIBILIDAD
INTEGRIDAD
INFORMACION PUBLICA
INFORMACION PUBLICA CLASIFICADA
INFORMACION PUBLICA RESERVADA
RIESGO

4. CONDICIONES GENERALES

Se debe realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad de la información, cuando se requiera otorgar acceso a los activos de información a los proveedores.

Antes de conceder los permisos de acceso a la información, el responsable del activo debe determinar: las necesidades del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso, los controles mínimos a tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información.

Antes de autorizar el acceso a la información a un proveedor se debe validar los antecedentes disciplinarios del proveedor conforme a los procedimientos establecidos por la Entidad.

En ningún caso se debe otorgar acceso a la información, sistemas de información o áreas seguras de la Entidad a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual y firmado el acuerdo de confidencialidad.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre El CPNAA y los proveedores se deben definir claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de clasificación; finalidad; autorizados para el tratamiento; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a la legislación vigente.

Los proveedores de servicios para la Entidad deben aceptar formalmente que cumplirán las políticas de seguridad de la Información de la entidad. En caso de conflicto entre las políticas de seguridad de la información del CPNAA y las políticas de seguridad de la información del proveedor, el supervisor del contrato debe coordinar la aprobación de un acuerdo de seguridad de la información para el contrato. Una vez aprobado el acuerdo, los responsables de la supervisión de los contratos deben realizar seguimiento a los compromisos y comunicar al Profesional Universitario Código 02 Grado 03 de la Oficina Administrativa y Financiera de cualquier evento de seguridad relacionado con los proveedores.

Se debe comunicar al proveedor el esquema de clasificación de información definido por la Entidad, en caso de diferencias entre los esquemas de clasificación de información de la Entidad y del proveedor primará el nivel de clasificación de la Entidad cuando se trate de información definida como pública en el Decreto 1081 de 2015 Decreto

Reglamentario Único del Sector Presidencia de la República, ley general de archivo, ley 1581 de 2012 y demás regulación estatal en materia de control de acceso a la información pública.

El proveedor debe aceptar la implementación de controles de seguridad razonables que protejan la información de la Entidad que quede bajo su responsabilidad. El proveedor debe aceptar el derecho de la entidad de realizar seguimiento, revisión y evaluación de la efectividad de las medidas de seguridad acordadas para proteger la información de la Entidad.

Los supervisores de contrato deben comunicar a los proveedores las reglas de uso aceptable y las prohibiciones sobre el uso de información de la Entidad para fines diferente al cumplimiento del contrato.

Los equipos y software que utilice el proveedor para el desarrollo de sus actividades, deben cumplir con los requisitos del subsistema de gestión de seguridad de la información de la Entidad, incluidos, derechos de autor, controles contra código malicioso, control de acceso y los demás controles acordados con la Entidad.

Los proveedores a cargo de actividades que involucran cambios en la configuración de los equipos de tecnología de información y comunicaciones de la Entidad, deben asegurar mediante los procedimientos de control de cambios, la correcta instalación y pruebas que aseguren el buen funcionamiento y la protección de la seguridad de la información de los activos de información de la Entidad.

El proveedor no está autorizado a usar los recursos de información y tecnología y la información de la Entidad para fines diferentes a los especificados en los contratos suscritos con la Entidad.

El uso de las redes de telecomunicaciones de la Entidad, solo está autorizado para el cumplimiento del objeto contractual suscrito, no está autorizado el uso de las redes de la Entidad para descargas de material protegido por derechos de autor (música, video, software, libros).

El proveedor no está autorizado a conectar, desconectar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización del supervisor del contrato.

El proveedor no está autorizado a instalar o ejecutar programas que perjudiquen la estabilidad de los equipos, su sistema operativo o sus programas internos o aplicaciones de la Entidad. Esto incluye los programas conocidos como virus informáticos, cualquier tipo de ensayo o experimento, hardware, software o cualquier software considerado como malicioso.

Cuando el proveedor tenga conocimiento o sospecha de la ocurrencia de eventos o incidentes de seguridad de la información que puedan afectar los activos de información de la Entidad, debe reportar la situación al Profesional Universitario Código 02 Grado 03 de la Oficina Administrativa y Financiera

DEFINICIÓN

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados
DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000:2014)
INFORMACION PUBLICA: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, Ley 1712/2014.
INFORMACION PUBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712/2014
INFORMACION PUBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014
INTEGRIDAD: La propiedad de salvaguardar la exactitud y complejidad de la información. (Norma ISO27000:2014)
RIESGO: Toda posibilidad de ocurrencia de aquella situación que pueda afectar el desarrollo normal de las funciones de la entidad y el logro de sus objetivos.

CONSEJO PROFESIONAL NACIONAL DE ARQUITECTURA Y SUS PROFESIONES AUXILIARES

POLÍTICA RELACIONES CON PROVEEDORES

Código	PA-GC-11
Versión	1
Tipo	Politica
Implementación	13/09/2017
Alcance	
Nivel de confidencialidad	

ELABORÓ	REVISÓ	APROBÓ
FELIX ALBERTO ROZO LARA **PROFESIONAL UNIVERSITARIO CODIGO 02 GRADO 03 - OFICINA ADMINISTRATIVA Y FINANCIERA** **Fecha de elaboración:** 09/08/2017	FELIX ALBERTO ROZO LARA **PROFESIONAL UNIVERSITARIO CODIGO 02 GRADO 03 - OFICINA ADMINISTRATIVA Y FINANCIERA** **Fecha de revisión:** 10/08/2017	DIANA FERNANDA ARRIOLA GOMEZ **DIRECTORA EJECUTIVA CODIGO 01 GRADO 03** **Fecha de aprobación:** 13/09/2017