

	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Fecha	27-09-2019
		Página	1 de 4



REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN QUE DEBEN CONTEMPLAR LOS CONTRATOS CON PROVEEDORES

Elaborado por: Unidad de Informática	Revisado por: Encargado de Seguridad de la Información	Aprobado por: Comité de Seguridad de la Información
--	--	---

	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Fecha	27-09-2019
		Página	2 de 4

INDICE

I. INTRODUCCIÓN 3

II. OBJETIVO..... 3

III. REQUISITO DE SEGURIDAD DE LA INFORMACIÓN QUE DEBEN CONTEMPLAR LOS CONTRATOS CON PROVEEDORES DE BIENES Y SERVICIOS 3

IV. DIFUSIÓN Y REVISIÓN 4

	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Fecha	27-09-2019
		Página	3 de 4

I. INTRODUCCION

Este documento se basa en el objetivo de control A.15 "Relación con los proveedores" que, a su vez, se especifica en el punto decimo quinto de los dominios de la NCH ISO 27001:2013. El presente documento trata específicamente el Control A.15.1.2 "Abordar la seguridad dentro de los acuerdo con los Proveedores".

El presente control tiene por finalidad establecer que las condiciones de seguridad de la información deben quedar reflejadas en los contratos de forma explícita y en un apartado específico para ello.

II. OBJETIVO

El presente documento establece los requisitos y compromisos relativos a la Seguridad de la Información, que deben cumplir los proveedores de servicios y bienes de la Institución en consideración de la naturaleza y particularidades de cada contratación, lo que deberá ser difundido para su respectivo cumplimiento a todas las áreas responsables de la adquisición y/o contratación de recursos tecnológicos.

III. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN QUE DEBEN CONTEMPLAR CONTRATOS CON PROVEEDORES DE BIENES Y SERVICIOS

Los contratos sobre bienes y servicios deben incluir entre sus condiciones contractuales cláusulas de confidencialidad respecto de la información a la que puede acceder un proveedor con ocasión de la prestación del servicio contratado o de la utilización del bien adquirido, aun cuando haya finalizado la vigencia de la respectiva contratación. La cláusula referida es indispensable si se trata de datos personales.

En razón de lo anterior, y en atención a la naturaleza de la contratación, en el pliego de condiciones que rige la contratación se deberá exigir que el proveedor designe a un responsable de seguridad de la información, quien servirá de interlocutor para cualquier tema asociado a dicha materia y será el responsable de que se cumplan los compromisos pactados entre la Subsecretaría de Justicia y el proveedor.

Asimismo, entre las condiciones contractuales se deberá disponer la obligación de mantener informada a la Subsecretaría de Justicia de cualquier cambio de personal asignado por el proveedor para la prestación de los servicios contratados.

Los contratos que tengan por objeto la instalación y mantenimiento del hardware y software deberán incluir cláusulas de propiedad intelectual estableciéndose claramente la propiedad de los materiales preexistentes que aporta cada parte para la prestación de los servicios contratados y/o bienes adquiridos.

Si el personal del proveedor contratado requiere acceso a los sistemas de la Institución, el pliego de condiciones que regula la contratación deberá establecer un procedimiento para

	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Fecha	27-09-2019
		Página	4 de 4

ello, indicado el tipo de información, sistemas, equipos y lugares sobre los que se autoriza y/ o prohíbe el acceso por parte del proveedor y de sus dependientes.

Para incentivar el cumplimiento de los términos contractuales, el pliego de condiciones deberá contemplar medidas de incumplimiento objetivas en consideración de la naturaleza del servicio contratado y/o bien adquirido que serán aplicables a través de los procedimientos dispuestos en el pliego para dicho efecto.

Finalmente, el pliego de condiciones de cada contratación deberá establecer claramente que la Subsecretaría de Justicia estará facultada para auditar, monitorear y supervisar las actividades que involucren información reservada, en especial respecto de las unidades clasificadas como “de riesgo”, tales como Informática, Recursos Físicos, Gestión y Desarrollo de Personas y Departamento de Presupuesto y Finanzas, entre otras.

IV. DIFUSIÓN Y REVISIÓN

El presente documento se difundirá a los usuarios de la Subsecretaría de Justicia, a través de correo electrónico Institucional.

Anualmente se realizará una revisión del presente documento y en caso de ser necesario se gestionará una actualización del mismo conforme a los procedimientos y normativa vigente aplicable.