Fecha: DD_____/ MM_____/ AA_____ Ciudad / Lugar:

_____

Grado, Nombres y Apellidos: _____ Identificación:

_____

Unidad: _____ Área: _____ Grupo:

_____

No	COMPROMISOS CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	NO CUMPLE
1	Cumplimiento a los controles de escritorios y pantallas limpios.	
2	Instalación y utilización únicamente de software licenciado y/o autorizado por la Oficina de Telemática, en los equipos de cómputo institucionales.	
3	Utilización de dispositivos de almacenamiento masivo autorizados por el Jefe de Telemática o Analista de Seguridad de la Información en la plataforma tecnológica institucional.	
4	Extracción de equipos de cómputo institucionales de las instalaciones policiales, con autorización del Jefe de Telemática o Analista de Seguridad de la Información.	
5	Conexión de computadores portátiles u otros dispositivos electrónicos no institucionales a la red de datos de la Policía Nacional, con autorización del Jefe de Telemática o Analista de Seguridad de la Información.	
6	Uso adecuado de identidad policial digital (cuenta y contraseña de usuario empresarial).	
7	Apagado del equipo de cómputo asignado, en horas no laborales.	
8	Almacenamiento de información institucional en los equipos de cómputo institucionales o en el servidor de archivos, si se encuentra implementada esta herramienta.	
9	Acceso a carpetas o información de otras áreas o grupos con autorización del Jefe de Área, Grupo, Responsable de la misma o del Jefe de Telemática.	
10	Utilización de la red de datos de la Institución, evitando obtener, mantener o difundir material publicitario o comercial, así como distribución de mensajes masivos.	
11	Autorización de ingreso de personas a las áreas restringidas y/o lugares en los que se procese información sensible con la autorización correspondiente.	
12	Almacenamiento seguro y/o bajo llave de documentos impresos que contengan información institucional, al terminar la jornada laboral o cuando no se haga uso de la misma.	
13	Cuidado con la información institucional y conservación de medidas apropiadas de seguridad para garantizar su protección.	
14	Ingreso a la infraestructura tecnológica de la Policía Nacional a través del servicio de acceso remoto utilizando el servicio VPN (virtual prívate network) previa autorización de la Oficina de Telemática	
15	Utilización adecuada de los recursos tecnológicos institucionales, para actividades propias del servicio policial y en beneficio de la Policía Nacional.	
16	Acatamiento de normas de seguridad industrial evitando comercializar, comer y/o beber cualquier tipo de alimento, cerca a los equipos de cómputo.	
17	Creación de páginas web, blog o sitios únicamente autorizados, para la publicación de documentos y promoción de servicios establecidos por la Institución.	
18	Otorgamiento de privilegios de acceso a los activos de información a funcionarios o terceros autorizados.	
19	Realización de cambios en la Plataforma Tecnológica de la Policía Nacional, con autorización de la Oficina de Telemática.	
20	Protección a la reputación o imagen de la Policía Nacional o alguno de sus funcionarios	

No	COMPROMISOS CON EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	NO CUMPLE
	desde la Plataforma Tecnológica de la Institución o fuera de ella.	
21	Difusión de información clasificada de la Policía Nacional a personas o entidades autorizadas.	
22	Cuidado de elementos y/o dispositivos tecnológicos, entregados para actividades propias del servicio policial.	
23	Cierre o bloqueo de sesión y/o exposición de información a cargo del funcionario, durante ausencias del puesto de trabajo.	
24	Clasificación de la información de acuerdo a la normatividad vigente.	
25	Protección de la información en los equipos que se autorizan fuera de las instalaciones empleando cifrado ó claves robustas para ingreso y claves a los documentos contenidos en él mismo.	
26	Utilización de privilegios como administrador, únicamente para actividades propias del servicio, en pleno cumplimiento de la normatividad vigente y una vez sean diligenciado los formatos establecidos en la suite visión empresarial.	
27	Utilización de dispositivos de almacenamiento masivo en los equipos institucionales cuya autorización ha sido otorgada por el Jefe de Telemática, Analista de seguridad de la información o centros de protección de datos.	
28	Utilización de computadores portátiles, tabletas, agendas electrónicas, teléfonos y demás dispositivos personales en las instalaciones policiales, únicamente los autorizados por el Jefe de Telemática, Analista de seguridad de la información o centros de protección de datos.	
29	Inclusión de los equipos o dispositivos de cómputo institucionales asignados para el servicio, dentro del dominio respectivo, con los controles necesarios para proteger la información allí alojada o a la que se pueda tener acceso a través del mismo.	
30	Firma de acuerdos de confidencialidad y demás documentos esenciales para el cumplimiento de la política de seguridad de la información de la Policía Nacional antes de tener cualquier tipo de acceso a la infraestructura tecnológica de la institución.	
31	Reporte de novedades tales como: licencias, vacaciones, excusas de servicio, traslado, retiro, desaparición, secuestro, para bloquear las cuentas de acceso a los recursos tecnológicos, sistemas de información y/o acceso a instalaciones.	
32	Realización de borrado seguro al reasignar o dar de baja un equipo de cómputo o cualquier dispositivo de almacenamiento.	
33	Confidencialidad en carpetas físicas y/o digitales, que contienen información en las estaciones de trabajo.	
34	Utilización de la infraestructura tecnológica de la policía nacional para acceder únicamente a la red o servicios de internet autorizados.	
35	Cumplimiento a los controles de acceso físico a instalaciones policiales. (validación biométrica, carné, acompañamiento de visitantes)	
36	Cumplimiento a los controles de seguridad establecidos en el Sistema de Gestión de Seguridad de la Información.	
37	Cumplimiento con las políticas establecidas para los servicios establecidos de la ECD (Entidad de Certificación Digital),	
38	Otras (relacionadas con los protocolos de seguridad de la información establecidos en cada unidad)	

Documento adjunto: _____. Ejemplo:(informe, fotografías, videos).

De acuerdo a lo contemplado en la Ley 1015 de 2006 "Régimen Disciplinario para la Policía Nacional", Ley 1273 de 2009 "Protección de la Información y de los datos", Ley 1581 del 2012 “Protección de datos personales” y al Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional, yo_____ identificado con C.C. No._____, reitero mi compromiso de cumplir los lineamientos establecidos en la normatividad referida.

Por tanto, se deja constancia de que el incumplimiento a las políticas de seguridad de la información de la Policía Nacional, implicará acciones de tipo penal, disciplinario, administrativo y/o fiscal.

_____ Firma y post-firma funcionario notificado

_____ Firma y post-firma funcionario notificador