Yo _____ identificado con Cédula de Ciudadanía No _____de _____obrando como Contratista (__) o Funcionario (__) o Pasante (__) y ejerzo mis funciones y/o obligaciones contractuales en la dependencia_____, me comprometo a cumplir las siguientes políticas y recomendaciones de seguridad:

CONOCIMIENTO DEL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN

Conocer y cumplir el M-PG-07 Manual Operativo de seguridad de la información[1] y la normativa de derechos de autor[2]. Presentar la evaluación de conocimiento de seguridad de la información, hasta que el resultado sea aprobado. Participar en la identificación de activos y riesgos de seguridad de la información de la dependencia. Reportar al Centro de Servicios (centrodeservicios@dnp.gov.co) los incidentes, anomalías, correos maliciosos, sospechosos y solicitudes de TIC.

USO DE LAS CONTRASEÑAS DE LOS SISTEMAS, PORTALES APLICATIVOS, CORREO INSTITUCIONAL, ACCESO A COMPUTADORES INSTITUCIONALES Y ACTIVOS TIC.

Proteger la confidencialidad de las contraseñas entregadas en el ejercicio de las actividades porque son personales e intransferibles. No dejar la información confidencial y contraseñas de sistemas, portales aplicativos, correo institucional, acceso a computadores institucionales y activos TIC al alcance de otras personas. No prestar las contraseñas. Cambiar las contraseñas con periodicidad, por lo menos cada dos meses. Cuando cambie la contraseña no utilizar las que se hayan usado previamente, será significativamente diferente de otras contraseñas anteriores, tendrá al menos siete (7) caracteres, usará combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales como: ¡!"#$%&&/()=?¡><[*], no usará nombres propios de personas, mascotas, equipos deportivos, ni fechas, ni similares, no usará caracteres repetidos (por ejemplo: AAAA, xxx, etc.)., caracteres incrementales, por ejemplo: MARIA1, MARIA2 y no tendrá significado obvio que permita su fácil deducción e identificación.

USO DE CORREO

No enviar información del DNP a través de cuentas de correo no institucional, o herramientas no institucionales. No utilizar la cuenta institucional para trámites personales, bancarios y/o comerciales. No suscribirse en boletines en línea, con el correo institucional, esto evita la llegada de cadenas de correo, publicidad, etc. No enviar correos electrónicos masivos con fines no institucionales. No enviar de cadenas de correo. No responder mensajes donde le solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. No enviar o reenviar correos electrónicos con contenido difamatorio, ofensivo, racista u obsceno. No generar o transmitir mensajes que puedan afectar de cualquier manera la imagen, dignidad y buen nombre de terceras personas o del DNP. No adulterar los mensajes de correo. (Por ejemplo: cambiar el campo de identificación de quien origina el correo). No está permitido enviar mensajes de correo

USO DE LAS ESTACIONES DE TRABAJO

No dejaré la estación de trabajo con la sesión abierta. Cuando retire del DNP activos (portátiles, discos duros, equipos de cómputo, otros equipos electrónicos) seré responsable de la custodia, salvaguarda de la información que allí este almacenada. Registraré en la portería de los edificios donde están las oficinas del DNP los equipos personales que ingresen a las instalaciones. Estaré atento a los equipos personales que ingrese al DNP, porque en caso de pérdida el DNP no se hace responsable. Reportaré de forma inmediata a la Subdirección Administrativa (SA) el extravió o hurto de los equipos del DNP. Cuando requiera compartir información con usuarios internos, externos y/o entidades usaré las herramientas institucionales que son SharePoint y One Drive. Estar atento a las transacciones financieras realizadas en los equipos institucionales ya que la Entidad no se hace responsable por el resultado de transacciones financieras personales que se realicen desde los equipos institucionales. Usaré los equipos institucionales con propósitos laborales. No almacenaré información de carácter personal o no institucional en los equipos del DNP, y en los discos de red. Haré un buen uso del internet para no afectar el oportuno y eficiente cumplimiento de las funciones asignadas, ni la obligación de dedicar la jornada laboral a la realización de tales funciones. La navegación y descarga de archivos en Internet la realizaré de forma razonable y con propósitos laborales. Mantendré la configuración establecida por la Oficina de Tecnologías y Sistemas de Información (OTSI) (Ej.: mecanismos de protección antivirus y la activación de un firewall en el equipo portátil). No descargaré software de internet u otro servicio en línea en cualquier equipo del DNP sin autorización de la Oficina de Tecnologías y Sistemas de Información. Revisaré que todos los medios extraíbles sean verificados con un antivirus del DNP, antes de procesarlos en equipos de la Entidad. No manipularé las impresoras, equipos de cómputo, u otro elemento tecnológico propiedad del DNP, en caso de presentarse problemas y/o fallas los reportaré al Centro de Servicios. Apagaré los activos de Información tecnológicos (estaciones cliente, portátiles, monitores, televisores e impresoras) al finalizar la jornada.

PROTECCIÓN DE DATOS PERSONALES

Usar para la creación de formularios de recolección de información, las herramientas institucionales son SharePoint o Forms de Office 365. En caso de requerir realizar una encuesta que por motivos laborales recolecte datos personales, comunicarse con la OTSI para recibir orientaciones en el cumplimiento de la Política de datos personales del DNP. Conocer y cumplir con el M-PG-12 Manual para la Política de Tratamiento de la Información de Datos Personales en el DNP[4]. El correo electrónico institucional está protegido por la normativa de datos personales, por ello debe solicitar copia del correo electrónico institucional a la OTSI previo al retiro de la Entidad y entregarlo al jefe directo en la dependencia.

USO DE LA INFORMACIÓN INSTITUCIONAL

Almacenaré la información institucional en la plataforma tecnológica del DNP (discos de red o sistemas de información o aplicativos o portales o One Drive o SharePoint empresariales) según corresponda y que tenga relación con el ejercicio de las funciones o actividades contractuales. Usaré para la creación de formularios de

[1] https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx

[2] https://colaboracion.dnp.gov.co/CDT/DNP/SIG/Anexo%201%20-%20Normograma%20y%20otros%20documentos%20de%20origen%20externo.xlsx

[4] https://intranet.dnp.gov.co/SGC/Procesos-Estrategicos/Paginas/direccionamiento-estrategico.aspx

utilizando la cuenta de correo de otra persona exceptuándolos casos aprobados por la OTSI. Eliminar todo correo de origen desconocido o de dudosa procedencia. No abrir mensajes o documentos adjuntos que no tienen una relación con las actividades del DNP. En caso de requerir el envío de correos con tamaño superior a 35 MB debe solicitar el permiso a la OTSI.

USO DE LAS REDES SOCIALES

No usar el correo institucional para la creación de cuentas en redes sociales como Twitter, Facebook, Instagram, LinkedIn, YouTube, Flickr y similares. Los voceros oficiales en las redes sociales del DNP son designados únicamente por la Dirección General del DNP.

RESPONSABILIDADES PARA LOS LIDERES TECNICOS DE APLICATIVOS, PORTALES Y SISTEMAS DE INFORMACIÓN

Almacenar los programas fuentes en el repositorio de código Microsoft DevOps Server de la OTSI. Cumplir con el M-TI-01 Manual Operativo para la Implementación y Mantenimiento de Sistemas de Información[3].

USO DEL TOKEN DE FIRMA DIGITAL

Seré responsable de todas las transacciones y acciones efectuadas con el token asignado. No firmar utilizando el token de otra persona. Informar a la OTSI la pérdida de token de firma digital u olvido de la contraseña.

USO DE LOS PUESTO DE TRABAJO

Mantener con llave los archivadores y escritorios que le sean asignados. Almacenar los documentos confidenciales en los archivadores y escritorios asignados al finalizar el día o si se va a ausentar del puesto de trabajo. No dejar documentos confidenciales a la vista y/o acceso de otras personas. Destruir los documentos confidenciales antes de ser arrojados en las canecas de reciclaje. Recoger de forma inmediata los trabajos de impresión que contengan información confidencial. Mantener organizado y en orden el puesto de trabajo asignado. No ingerir alimentos ni bebidas en el puesto de trabajo con el fin de evitar riesgos en los activos tecnológicos.

recolección de información, las herramientas institucionales que son SharePoint o Forms de Office 365. No divulgaré y/o publicaré información digital y/o almacenada en los discos de red, y/o sistemas de información propiedad del DNP, sin expresa autorización del jefe inmediato. No usaré la información institucional con fines lucrativos o comerciales. No venderé, transferiré, intercambiaré información institucional con terceros para propósitos diferentes a cumplir con la misión del DNP, sin expresa autorización del jefe inmediato. No enviar información clasificada5 y/o reservada6 del DNP a personas u organizaciones externas, si estar autorizado para ello. No reenviar o copiar sin permiso mensajes "confidenciales"7 o protegidos por las normas sobre derechos de autor, o contra expresa prohibición del originador.

PERSONAL A SU CARGO

Promover que el personal a cargo conozca y cumpla el M-PG-07 Manual Operativo de seguridad de la información. Gestionar que personal a cargo presente la evaluación de conocimiento de seguridad de la información, hasta que el resultado sea aprobado. Informar a la Subdirección de Gestión y Desarrollo del Talento Humano y/o al Grupo de Contratación cuando el personal a su cargo termine su relación laboral o contractual, y/o sea trasladado a otra dependencia. Cuando una persona a su cargo se encuentre ad-portas de terminar su relación laboral o contractual con la entidad, el jefe de área responsable y/o supervisor del contrato, deberá informar con una antelación mínima de 8 días hábiles a la fecha de finalización del referido vínculo, a los líderes funcionales y técnicos, administradores de los sistemas de información según corresponda y a la OTSI; con el fin de proceder a retirar los accesos lógicos de ingreso a los activos de información a los que el usuario tenía acceso. En caso de requerir la copia de seguridad del equipo de cómputo de la persona a su cargo deberá informar a la OTSI con una antelación mínima de 8 días hábiles a la fecha de finalización del referido vínculo. Verificar la entrega de la información, su organización en los discos de red cuando el personal a su cargo termine su relación laboral o contractual, y/o sea trasladado a otra dependencia. Verificar que los activos asignados a los funcionarios, contratistas, pasantes o proveedores sean devueltos a la Subdirección Administrativa cuando el personal a cargo termine su relación laboral o contractual, y/o sea trasladado a otra dependencia.

Fecha: __-___-____ Nombre: _____ Firma: _____

[3] https://intranet.dnp.gov.co/SGC/procesos-apoyo/Paginas/gestion-de-tic.aspx

[5] **Información Clasificada:** Pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, derechos particulares o privados consagrados en el artículo 18 de ley 1712 de 2014. Art 18. a) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado por el artículo 24 de la Ley 1437 de 2011. b) El derecho de toda persona a la vida, la salud o la seguridad. c) Los secretos comerciales, industriales y profesionales.

[6] **Información Reservada:** Información exceptuada por daño a los intereses públicos. a) La defensa y seguridad nacional; b) La seguridad pública; c) Las relaciones internacionales; d) La prevención, investigación y persecución de los delitos y las faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos, según el caso; e) El debido proceso y la igualdad de las partes en los procesos judiciales; f) La administración efectiva de la justicia; g) Los derechos de la infancia y la adolescencia; h) La estabilidad macroeconómica y financiera del país; i) La salud pública, i) opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos.

[7] **Confidencial o de reserva:** Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.