FOGACOOP
Fondo de Garantías de Entidades Cooperativas

POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD, PRIVACIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Mayo 2023

ESTA POLÍTICA ES DE OBLIGATORIO Y ESTRICTO CUMPLIMIENTO POR PARTE DE TODOS LOS EMPLEADOS DE FOGACOOP, LOS CONTRATISTAS Y TERCEROS QUE OBRAN EN NOMBRE DE FOGACOOP.

TODOS LOS EMPLEADOS Y CONTRATISTAS DEBEN OBSERVAR Y RESPETAR ESTA POLÍTICA EN EL CUMPLIMIENTO DE SUS FUNCIONES.

EL INCUMPLIMIENTO ORIGINA SANCIONES DE TIPO LABORAL O RESPONSABILIDAD CONTRACTUAL SEGÚN EL CASO.

Reglamento interno de trabajo Articulo 61. Obligaciones especiales del trabajador numeral 26. Cumplir con las normas establecidas para el control y prevención de lavado de activos y financiación del terrorismo (SARLAFT) y las medidas de prevención de riesgos de seguridad de la información y ciberseguridad, así como el código de buen gobierno y el código de conducta prescritos para la entidad, teniendo en cuenta que Fogacoop es una entidad vigilada por la Superintendencia financiera de Colombia, quien impone no solo el Cumplimiento de estas normas a nivel institucional sino también por parte de Cada uno de los trabajadores que laboren en el mismo.

Circular 04 de 2019 código de ética

Manual de funciones, ***numeral 7.4 Funciones y responsabilidades de todos los funcionarios del fondo y personal que labora para la entidad (todos los niveles jerárquicos de la entidad)***, apartado relacionado con la Gestión del riesgo, sub numeral 7. adoptar y poner en práctica las políticas de seguridad y privacidad de la información del fondo, y preservar la confidencialidad, integridad y disponibilidad de la información para garantizar su uso adecuado.
8. Adoptar las medidas de prevención y cuidado frente a los riesgos de ciberseguridad, atender recomendaciones e informar oportunamente sobre las amenazas de que sea objeto.

TABLA DE CONTENIDO

Pág.

1. **Objetivo** 4
2. **Alcance** 4
3. **Roles y responsabilidades** 4
4. **Políticas** 4
5. **Soporte políticas** 6
6. **Excepciones** 6

1. Objetivo

Garantizar que el software adquirido o desarrollado bien sea por terceras partes o directamente por el Fondo y su mantenimiento, incluya los controles de seguridad requeridos para la protección de la integridad, la disponibilidad y la confidencialidad de la información que va a administrar.

2. Alcance

Esta Política aplica a los supervisores de los contratos con los terceros que realicen desarrollos y mantenimiento a los aplicativos y al área de TI.

3. Roles y responsabilidades

A continuación, se describen los responsable, roles y responsabilidades de cada uno de los actores que tienen participación para el cumplimiento de la política descrita en este documento:

Responsable	Roles	Responsabilidades
Gerente de Riesgos	Seguridad de la Información	Debe definir lineamientos de buenas prácticas en seguridad de la información a terceros.
Gerencia de TI	Área de tecnología	Se asegurará de que las directrices entregadas en este documento sean cumplidas a cabalidad.
Supervisores y Líderes de proceso	Supervisores y Líderes de proceso	Garantizaran que el software adquirido desarrollado sea funcionalmente aceptable dentro de la necesidad del negocio.

4. Políticas

a. Todos los sistemas de información y/o comunicaciones que se adquieran o desarrollen deben tener una definición clara de los requerimientos funcionales, operacionales, especificaciones técnicas y criterios de aceptación, contemplando requerimientos de seguridad de la información. Este proceso deberá ser apoyado por los profesionales especialistas en la gerencia de TI y por el área usuaria que requiera la solución.

b. Garantizar que todos los desarrollos de los sistemas de información y/o comunicaciones estén completamente documentados y control de versionamiento. Igualmente, todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo en sitio externo a la entidad.

c. FOGACOOP desarrollará estrategias para asegurar que los sistemas de información incluyan condiciones de seguridad considerando los siguientes aspectos:

- No usar datos personales y sensibles en ambientes de prueba
- En caso de que los privilegios y perfiles asignados en los ambientes de pruebas sean más amplios a los que requiere en ambiente de producción, asegurarse de asignar en este último ambiente, los mínimos requeridos para el desarrollo de sus actividades.
- Procurar que la autenticación de los usuarios en las aplicaciones de uso interno se realice a través del directorio activo.
- Controlar la asignación de permisos según lo definido en el rol y/o perfil del usuario que ha sido solicitado y aprobado.
- Definir los mecanismos y controles que se requieran para administrar la información y asegurar su confidencialidad, disponibilidad e integridad, según la valoración que previamente se deba realizar de dicha información.
- Establecer los controles para la validación de los datos de entrada, para su procesamiento, para su almacenamiento y para las salidas de los datos, todo de acuerdo con los requerimientos funcionales y los requerimientos para su administración.
- Contar con ambientes de desarrollo, prueba y producción por separado.
- Aplicar metodologías probadas y estandarizadas para la creación de bases de datos adecuadamente estructuradas tanto para los ambientes en desarrollo como los de pruebas.
- Realizar para toda aplicación nueva, antes de entrar a producción y en etapa de pruebas, las respectivas pruebas de vulnerabilidad técnica y de seguridad de la información, estas dos últimas deben ser lideradas por la Gerencia de Riesgos.
- Realizar mantenimiento periódico y planificado a los sistemas de información y/o comunicaciones, para garantizar su correcto funcionamiento (depuración de usuarios, bases de datos, configuraciones, parámetros, entre otros y demás que resulten de incidentes).
- Introducir los cambios a los sistemas de información y/o comunicaciones, asegurando que dichos cambios son probados y documentados, controlando que dichos cambios tengan en cuenta la evaluación de los riesgos, se soporten e una definición de especificaciones, en pruebas de control de calidad y una adecuada gestión de su implementación que asegure la integridad del sistema.

- Todos los sistemas de información deben generar logs para seguimiento a las acciones y/o cambios ejecutados por los usuarios y administradores del sistema.

- Los responsables de seguridad de la información deben formar parte de los cambios cuando tenga una afectación a nivel de los pilares de la información.

- Gestionar adecuadamente los derechos de autor, propiedad intelectual, la confidencialidad que amerita la especificación del sistema y la información que administra y las normas aplicables al desarrollo de software en Colombia.

- Establecer lineamientos para la supervisión y seguimiento a las actividades de desarrollo seguro contratado, incluido la garantía de uso de técnicas de programación seguras y la implementación de condiciones de seguridad del ambiente de desarrollo, control y seguridad de los versionamientos, todo lo cual debe quedar inmerso en las cláusulas o especificaciones técnicas del contrato a ejecutar.

- Se debe definir lineamientos de buenas prácticas en seguridad de la información a terceros, que debe ser aceptado por el proveedor y debe ser un anexo a las obligaciones contractuales.

- Los responsables de seguridad de la información deben realizar análisis de riesgos de aquellos desarrollos que implique exponer información en internet, para identificar posibles brechas de seguridad y minimizar el riesgo de exposición de la información en internet.

5. Soporte políticas

Esta política será soportada por los siguientes instrumentos:

- Tecnología - PR-REIN-TI-004 Mantenimiento de Equipos de Computo

6. Excepciones

- La aplicación y desarrollo de los puntos descritos en la Política no excluye el cumplimiento de aquellas regulaciones y disposiciones legales y externas que le apliquen a la Entidad en esta materia.

- Cualquier excepción a esta política deberá tratarse de manera particular y deberá estar debidamente sustentada por el funcionario solicitante, y aprobada por el Subcomité de seguridad la información, gestión documental y arquitectura de datos. Deberá queda debidamente documentada en el Acta de la reunión en la que se presente la solicitud.

Historial de cambios

FECHA	ACTIVIDAD #	VERSIÓN	CAMBIOS
Abril 2012	----	1.0	Expedición de la política – versión inicial

FECHA	ACTIVIDAD #	VERSIÓN	CAMBIOS
Octubre 2016	No. 8.3 No. 11.1	2.0	Se ajustan los nombres de los cargos y áreas según la estructura actual del Fondo En el 8.3 se aclaró las acciones cuando los funcionarios están en vacaciones o licencia. En el 11.1 se incluyeron tres actividades adicionales relacionadas con la Administración de cuentas de usuario y contraseñas, conforme a la ISO 27001 numeral A.9.2.2.
Julio 2017	No. 10.6	3.0	Se desarrolla la política relacionada con el uso de periféricos y medios de almacenamiento removibles, precisando algunos de los controles que deben ser implementados por el Área de TI, contratación y funcionarios en general
Febrero 2018	Todo el documento	4.0	Incorpora la política general Actualiza las políticas con base en la ISO27001:2013 y su anexo A y en el Modelo de Seguridad y Privacidad de la Información de Mintic
Octubre 2022	Todo el documento	5.0	Se genera documento independiente por cada política y se realiza revisión y actualización de política. Se incluyen los instrumentos soportes de la política. Se hacen precisiones para realizar análisis de riesgos cuando se hace exposición de información en redes públicas.
Mayo 2023		6.0	Se actualiza la codificación por adopción del nuevo SGI