FOGACOOP
Fondo de Garantías de Entidades Cooperativas

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

POLÍTICA DE CONSTRUCCIÓN Y DESARROLLO DE SISTEMAS SEGUROS

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
4.1. Política de análisis y especificación de requerimientos de seguridad 4
4.1.1. Perfiles, Autenticación y Mecanismos de Cifrado 6
4.1.2. Validación de datos de entrada 7
4.1.3. Validación de datos de salida 7
4.1.4. Validación de procesamiento de datos 7
4.1.5. Integración entre sistemas 8
4.1.6. Validación de autenticación de mensajes 9
4.1.7. Validación de seguridad de código fuente y archivos 9
4.1.8. Validación de control de cambios en sistemas de información 9
4.2. Política de protección de datos de prueba 9
4.3. Política de control de versiones 10
4.4. Política de desarrollo externo de FOGACOOP 10
5. Excepciones 11

1. Objetivo

Presentar al equipo desarrollador los lineamientos y requerimientos de seguridad de la información en las actividades de construcción y desarrollo de aplicaciones para FOGACOOP.

2. Alcance

El alcance y enfoque de la política de construcción y desarrollo seguro incluye las actividades de desarrollo de aplicaciones al servicio de FOGACOOP.

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	Establecerá los lineamientos para trabajar con seguridad la construcción y los desarrollos que se realicen en la entidad
Gerencia de TI	Área de tecnología	Realizará la entrega y verificará el cumplimiento de los lineamientos establecidos en esta política por parte de los desarrolladores.

4. Políticas

a. Para las aplicaciones de la entidad y cualquier aplicación nueva que se desarrolle es necesario tener en cuenta controles de seguridad de acuerdo con la dinámica del negocio y el contexto en el que se desenvuelve.

b. Tener en cuenta que las aplicaciones contarán con los elementos de seguridad enunciados a continuación y los requerimientos sobre estos aplicativos ya tendrán inmersos dichas características de seguridad ya que es un proceso evolutivo.

4.1. Política de análisis y especificación de requerimientos de seguridad

a. Previo a que un sistema de información sea desarrollado, mantenido o adquirido, el responsable de la Seguridad de la Información en conjunto con TI, deberá especificar los requerimientos o necesidades de seguridad teniendo en cuenta el FOGACOOP, éste será un criterio fundamental para la aceptación del producto final.

b. Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean probados, revisados y recompilados.

c. Toda aplicación o sistema de información deberá tener en cuenta aspectos de seguridad de la información asociados a los perfiles de usuario y accesos sobre los procesos y datos a nivel transaccional y demás.

d. El paso a producción de cualquier aplicación implica una verificación de las normas de seguridad asociadas al sistema de información y deben pasar por control de cambios.

e. Teniendo en cuenta que los objetivos de la seguridad de la información serán la confidencialidad e integridad, todo desarrollo y/o adquisición deberá tener en cuenta dichos propósitos.

f. En ambiente de pruebas, se deberá verificar que las cuentas de usuario asignadas posean valor o importancia de la información ante un posible daño, divulgación o impactos que surja como resultado de fallas o por ausencia de la seguridad; por tanto, se adjuntará un listado de las necesidades de seguridad asociadas para la etapa de análisis y desarrollo del requerimiento o implantación del software.

g. La solicitud deberá ser evaluada con respecto a su viabilidad y conveniencia para analizar alternativas de desarrollo y la evaluación de los aspectos de seguridad necesarios en cumplimiento de los objetivos del requerimiento.

h. Se deben desarrollar pruebas de abuso (cargue y stress) verificando en todos los puntos los controles implementados, que aseguran la DISPONIBILIDAD de la información.

i. Desarrollar en todos los casos, previo a la puesta en producción; pruebas de aceptación con el objetivo de verificar si un sistema satisface los requisitos de la Entidad. Se debe ejecutar en toda la aplicación y se deben centrar en replicar las conductas de los usuarios. Para el caso de FOGACOOP, se deben revisar que los servicios se encuentren funcionando adecuadamente, previo a su publicación o puesta en producción.

j. Todo proyecto de desarrollo, mantenimiento o compra de software deberá cumplir los requisitos mínimos de seguridad y protección de la información de los accesos necesarios a las operaciones y a los datos, como actividad previa a implementación en ambiente de producción.

4.1.1. Perfiles, Autenticación y Mecanismos de Cifrado

a. Toda aplicación o sistema de información debe incluir el manejo interno de perfiles de usuario, accesos sobre tareas y los datos. Con la finalidad de asegurar que un usuario tenga los permisos necesarios para ejecutar su función y no se le concedan accesos y/o permisos a tareas que se excedan de su responsabilidad. En ese sentido la administración de perfiles y configuraciones de seguridad para las nuevas aplicaciones deben estar integrado con el módulo de administración de seguridad de FOGACOOP.

b. En caso de que no se puede realizar la integración con el módulo de administración de seguridad de FOGACOOP, se requiere que las aplicaciones cuenten con un módulo de manejo de perfiles de usuarios acceso sobre tareas y los datos, así mismo se requiere de módulo de autenticación que debe cumplir con:

   - Se debe manejar usuario personalizado y no genéricos en las aplicaciones.

   - Política de cambio de contraseña, con caducidad al menos cada 30 días. Cuando la aplicación requiera una excepción en el cumplimiento de este ítem, será revisando por el responsable de seguridad de la información

   - Funcionalidad de cambio de contraseña únicamente a usuarios autenticados validando la antigua contraseña, la nueva contraseña.

   - Bloqueo de la cuenta del usuario después de tres intentos fallidos.

   - Política de complejidad de contraseña (mínimo 8 caracteres, mínimo debe contar con una Mayúscula, un número, un carácter especial).

   - Se debe controlar que las últimas doce “12” contraseñas no sean reutilizadas.

   - Aplicar auto bloqueo a las aplicaciones por tiempo de inactividad “5 minutos”.

   - Aplicar controles Captcha para evitar ataques de negación de servicio por parte de robots.

c. Las conexiones de las aplicaciones que se encuentren expuestas a internet deben ser aseguradas con la versión más estable de protocolo TLS (HTTPS) o aquel que pueda reemplazarlo con un nivel de seguridad igual o mayor.

d. Las contraseñas de las aplicaciones almacenadas deben ser cifradas a través de algoritmos de cifrado robustos y bajo estándares de la industria, como SHA, AES, 3DES y RCA, con el fin que no sean fácilmente legibles en su almacenamiento o en el momento de la transacción. Existen diversas técnicas para el cifrado de contraseñas para suplir este requerimiento, se recomienda revisar y aplicar las librerías de java JCA, JCE o JCEF para cifrado en aplicaciones, esta última es la más completa en temas de cifrado en java a nivel de objetos y contraseñas.

e. Con el fin de proteger la confidencialidad e integridad de la información durante su transmisión a terceros o su almacenamiento, se deberá llevar a cabo una evaluación del riesgo de seguridad con el fin de identificar amenazas y controles de apropiados, dependiendo de la situación y/o de la criticidad de la información.

4.1.2. Validación de datos de entrada

a. Se debe asegurar la Validación de la información en su etapa de entrada en las aplicaciones para asegurar su integridad y minimización de la posibilidad de errores en la digitación para ingreso

b. Aplicar restricciones en las cajas de texto de las aplicaciones, con el fin de restringir el ingreso de meta caracteres como */%” ~ s/.*\&#(\d+);.*/$1/; y palabras reservadas de SQL, Oracle y java, para evitar inyección de código.

c. Las cajas de texto deben tener una longitud de caracteres limitada de acuerdo con el propósito, ejemplo: un campo cedula debe admitir un máximo de 15 caracteres numéricos y en el caso que se espere recibir cedulas de extranjería debería ser alfanumérica.

d. La aplicación debe garantizar que: “cuando se copie la URL del sitio, estando ya autenticado en los módulos de la aplicación y se copie en un nuevo navegador “la aplicación debe negar el acceso.

4.1.3. Validación de datos de salida

a. Se debe asegurar las validaciones de los datos de salida de modo que se garantice las ejecuciones correctas de acuerdo con los requerimientos funcionales solicitados y por ende los resultados esperados.

4.1.4. Validación de procesamiento de datos

a. Se deberá validar la información procesada por los programas de aplicación e incorporar puntos de verificación o Validación, para detectar posibles errores o problemas en los datos. Los controles específicos requeridos

dependerán de la naturaleza de la aplicación y del impacto causado por la alteración de datos.

b. Se deberán considerar los siguientes controles:

- Verificar la detección de los siguientes errores:
  - Valores fuera de rango
  - Caracteres inválidos en campos
  - Datos incompletos
  - Exceso de los límites máximos o mínimos de volumen de datos.
  - Validar extensiones de archivos que se suban a la aplicación.

- Revisiones periódicas del contenido de campos claves o archivos para confirmar su validez e integridad.

- Ejecutar los procedimientos apropiados para responder a la Validación de errores.

- Definir las responsabilidades de todo el personal involucrado en el proceso de digitación y en lo posible automatizar al máximo mediante documentos electrónicos.

4.1.5. Integración entre sistemas

La integración entre sistemas de información con terceros se deben considerar las siguientes estrategias, incorporando una o varias recomendaciones.

a. Integración mediante TCP/IP (Sockets)
   - Se debe realizar mediante una VPN o canal dedicado.
   - Se puede considerar cifrar el canal, pero esto degrada el desempeño en gran medida y ya no sería transaccional.

b. Integración mediante servicios SOAP o Se debe realizar mediante protocolo HTTPS.
   - Considerar tener un hash o checksum único.
   - Considerar exponer bajo una VPN o canal dedicado.
   - Considerar adicionar ws-segurity (Tener presente que esto demanda tiempo y complejidad en la transacción.)

c. Integración mediante servicios REST o Se debe realizar mediante protocolo HTTPS.
   - Considerar tener un hash o checksum único.
   - Considerar exponer bajo una VPN o canal dedicado.
   - Considerar adicionar JWT para el manejo de tokens y sesiones.

4.1.6. Validación de autenticación de mensajes

a. Para aquellos sistemas que comprendan la transmisión de datos sensibles y donde sea vital la protección de la integridad del contenido. (ej. transferencia de fondos de manera electrónica u otros intercambios de información) se debe realizar un análisis de riesgos para establecer la necesidad de establecer un sistema de autenticación de mensajes o protección de la data mediante cifrado.

4.1.7. Validación de seguridad de código fuente y archivos

a. Nuevas aplicaciones en desarrollo y sus datos, deberán ser estrictamente alojados en ambiente diferente a producción; esta separación se llevará a cabo a través de la separación de los directorios y las librerías en ambientes de desarrollo con control de seguridad.

b. En aquellas instancias donde el acceso al ambiente de producción es requerido para una modificación autorizada y/o para agregar una nueva aplicación, solo se concederán accesos de lectura y copiado a las personas que realizarán dicha actividad.

c. Código fuente de aplicaciones deberá ser respaldado y protegido en un lugar externo.

d. Las librerías de códigos fuentes de la Entidad deberán ser manejadas de manera centralizada y su acceso solo se realizará cuando se requiera una modificación o mantenimiento a una aplicación y mediante la puesta de una copia del código fuente a las librerías de ambiente de desarrollo.

4.1.8. Validación de control de cambios en sistemas de información

a. Todos los cambios significativos en aplicaciones, sistemas de información, o procedimientos críticos de producción, deberán ser solicitados formalmente a través del procedimiento de control de cambios se asegurará que sólo los cambios autorizados sean realizados y notificados al comité de cambios.

4.2. Política de protección de datos de prueba

a. Cuando las tareas de desarrollo y pruebas requieran datos de producción, se debe seleccionar un paquete de datos específicos y suficientes para su ejecución, de igual forma se debe garantizar que estos datos no contengan

información sensible del negocio o datos personales que afecten ley 1581 de Protección de datos personales.

b. Autorizar específicamente cada copia información operacional a un ambiente de pruebas.

c. Registrar las acciones para realizar el copiado y uso de la información operacional a través de log para suministrar un rastro de auditoría.

d. Aplicar los procedimientos de control de acceso, que se aplican a los sistemas de información operacionales, también a los sistemas de información de pruebas.

e. La información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.

4.3. Política de control de versiones

a. Antes de hacer uso de un nuevo aplicativo o con cambios sustanciales en ambiente de producción, deberá recibirse una aprobación escrita por parte de propietario de la información y/o responsable del área con la aprobación de su implementación en producción.

b. Las versiones del software deben ser protegidas para recuperación tanto por algún incidente o por requerimientos de información.

c. Cada actualización a la versión software crítico de FOGACOOP deberá ser actualizada y depositada en custodia del área de TI.

4.4. Política de desarrollo externo de FOGACOOP

a. Cualquier desarrollo de software contrata externamente deberá dar cumplimiento a las políticas y lineamientos descritos en este documento.

b. Todo proveedor que realice desarrollo para FOGACOOP deberá cumplir con todos los requisitos legales y acuerdo de confidencialidad correspondientes establecidos en FOGACOOP.

c. Todo Desarrollo deberá tener en cuenta y aplicar la política de Gobierno Digital emitida por el Gobierno Nacional para su cumplimiento normativo.

4.5. Seguridad de servicios de las aplicaciones en redes públicas

a. Cualquier servicio que vaya a exponer en redes públicas (internet) deberá estar protegidos por mecanismos de seguridad Informática como Firewall, IPS, WAF.

b. El responsable del servicio a exponer en conjunto con la Gerencia de TI y el responsable de Seguridad de la Información deberán realizar en un análisis de Riesgos al servicio a exponer en redes públicas para determinar los controles de seguridad que se deben implementar.

c. El Gerente de TI junto con el responsable de Seguridad de la información serán los responsables de autorizar la publicación de los servicios en redes públicas (Internet).

d. Cualquier servicio que se vaya a exponer en internet deberá contar con un análisis de vulnerabilidades previo, las vulnerabilidades identificadas deberán ser remediadas antes de su publicación en rede públicas (Internet)

5. 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
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

FECHA	ACTIVIDAD #	VERSIÓN	CAMBIOS
			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 definieron de manera detallada los lineamientos de seguridad para la construcción y el desarrollo seguro.
Mayo 2023		6.0	Se actualiza la codificación por adopción del nuevo SGI