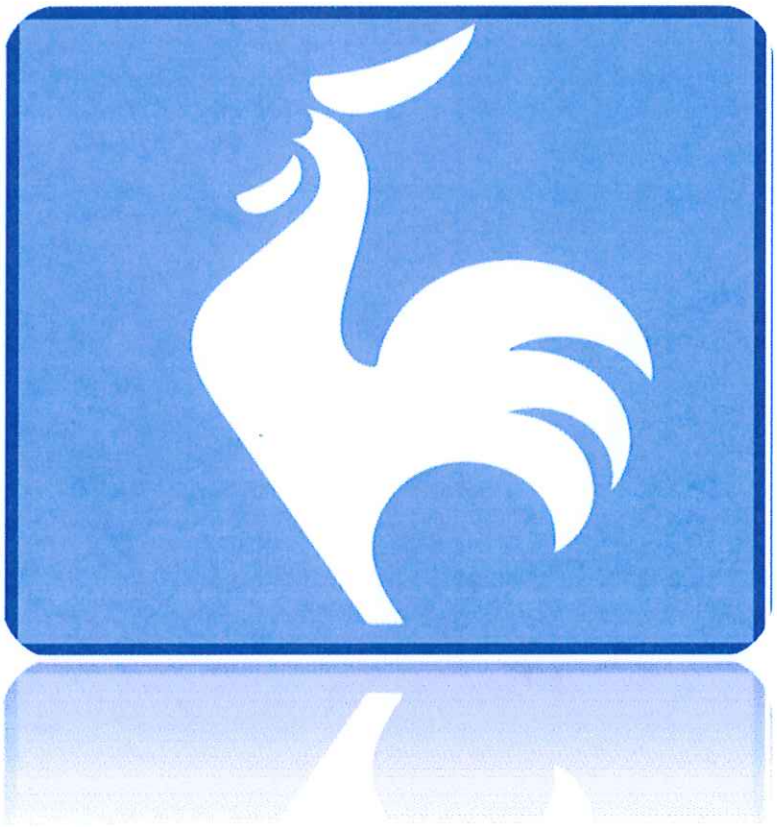
# FCPC DE JUBILACIÓN Y CESANTÍA DE LOS SERVIDORES DE LA SUPERINTENDENCIA DE BANCOS



# POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

## 1. INTRODUCCIÓN

Para dar cumplimiento al proceso de modernización los controles del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos aprobó el presente documento.

Para los efectos de esta política, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.

Este documento no trata de una descripción técnica de mecanismos de seguridad ni de una expresión legal que involucre sanciones a conductas de los funcionarios. Es más bien una descripción de lo que se desea proteger, el porqué de ello y quién está involucrado.

## 2. OBJETIVO

La presente política tiene como objetivo, proporcionar seguridad razonable con respecto a la integridad y seguridad de los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas del usuario y los derechos y privilegios asociados con ellas, para acceder a los servidores, aplicaciones, bases de datos y a las instalaciones de procesamiento de la información a través de:

- Adecuado manejo y mantenimiento de las cuentas de usuario y los derechos y privilegios asociados a ellas.
- Adecuado manejo y mantenimiento de certificados digitales, incentivando su uso.
- Buenas prácticas de usuarios de red.
- Control de acceso a los servicios de red internos con restricción de la instalación de equipamiento personal y mantención de catastro de equipamiento y personas con privilegios de acceso.
- Instructivos relativos a uso de redes y servicios de red.

## 3. ALCANCE

Esta política aplica a todos los sistemas del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos, incluyendo sin limitar a las aplicaciones comerciales, bases de datos, aplicaciones desarrolladas internamente, equipos, instalaciones, sistemas, y redes que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger los activos de información que se encuentren en otras formas.

Abarca todos los activos de información que el FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos posee en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas. La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

## 4. DEFINICIONES

**Activo:** Es toda información que tenga valor para la organización. Una organización incluye diferentes tipos de activos: activos relacionados con el entorno (edificios, instalaciones, equipamiento) y personal, activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones), activos relacionados con la información (datos, soporte), activos relacionados con las funcionalidades de la organización (productos, servicios) y activos intangibles (credibilidad, conocimiento acumulado).

**Custodio de la información:** Es cualquier persona que mantiene bajo su responsabilidad información de la cual no es el Propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos.

**Incidente de seguridad:** Situación adversa que amenaza o pone en riesgo un sistema.

**Información:** Contenido de un documento. Ejemplos de tipos de información:

- **Reservada:** Calidad de un acto, resolución, fundamento, procedimiento o documento que le permite ser conocido únicamente en el ámbito de la unidad del órgano a que sean remitidos, tales como división, departamento, sección u oficina
- **Secreta:** Calidad de un acto, resolución, fundamento, procedimiento o documento que le permite ser conocido sólo por las autoridades o personas a las que vayan dirigidos y por quienes deban intervenir en su estudio o resolución.

**Negocio:** Función o servicio prestado por la organización.

**Política de seguridad:** Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés para la organización, o bien garantizar la realización periódica y sistemática de este conjunto.

**Propietario de la información:** Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.

**Riesgo:** Probabilidad de ocurrencia de un evento indeseado con consecuencias negativas.

## 5. RESPONSABILIDADES

**Comité de Seguridad de la Información:** En su calidad de tal, responde ante la Administración del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos y del cumplimiento de las medidas orientadas a mantener un nivel de seguridad de la información acorde con las necesidades del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos y los recursos disponibles.

**Encargado de Seguridad de la Información (ESI) u Oficial de Seguridad de la Información (OSI):** Es el representante del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos en la definición y aplicación de los criterios de seguridad de la información en el FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos, será responsable de velar por el fiel cumplimiento de la política de seguridad, sus normas, procedimientos y estándares.

**Personal del Fondo:** Tiene la responsabilidad de cumplir con lo establecido en este documento y aplicarlo tanto en su entorno laboral, como fuera de éste. Además, tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

## 6. POLÍTICAS

6.1 Los funcionarios sólo pueden acceder a visualizar y/o trabajar aquella información para la que están expresamente autorizados por el dueño del activo o el proceso.
6.2 Ningún usuario debe descargar programas utilitarios sin el visto bueno de Plataforma TICs.

6.3 Todos los requerimientos de información de la organización que incluyan, sin limitar, comunicados públicos, declaraciones, cuestionarios, encuestas o entrevistas periodísticas, deben ser referidos a la Unidad de Comunicaciones del ISP.
6.4 Se deben establecer procedimientos formales para el registro y eliminación de usuarios, de modo de garantizar que se otorguen y quiten accesos a los sistemas y servicios de información, en consistencia con los niveles de autorización de los usuarios.
6.5 Se deben revisar los derechos de acceso otorgados a los usuarios regularmente a través de procedimientos formales.
6.6 Cuando un empleado deja algún puesto en la organización, los archivos residentes en los computadores y los archivos impresos deben ser revisados por su supervisor o el jefe inmediato, para una inmediata reasignación formal de obligaciones y responsabilidades.
6.7 Los funcionarios de la organización no deben utilizar herramientas para obtener información de la red, como detección de puertos, servicios y archivos en general en los sistemas de información de la organización.
6.8 El acceso lógico a la configuración de puertos de manera remota debe ser controlado.
6.9 Para los accesos a sistemas se deben establecer procedimientos de autenticación seguros, de modo de minimizar la oportunidad de accesos no autorizados.
6.10 No se deben utilizar cuentas genéricas para acceder a los sistemas y aplicaciones del Fondo.
6.11 Todos los usuarios deben autenticarse con User y Password válidos antes de usar sistemas de información del FCPC SB.
6.12 Los funcionarios de áreas técnicas no deben utilizar ninguna estructura de contraseña que resulte predecible o fácil de adivinar, esto incluye sin limitar, a contraseñas en blanco, palabras que aparezcan en diccionarios, secuencias comunes de caracteres y datos personales. Las contraseñas fijas no deben ser almacenadas en archivos de ejecución por lotes, scripts automáticos, macros de software, computadoras de control de acceso o en otros medios donde personas no autorizadas pueden conocerlas.
6.13 Las contraseñas no deben ser escritas o almacenadas en lugares visibles o cerca de los sistemas a los cuales permiten el acceso.
6.14 Todos los funcionarios de la organización, deben dejar siempre sus equipos bloqueados en caso de no estar en su lugar de trabajo.
6.15 Todos los Equipos de trabajo del personal de ISP deben estar configurados con protector de pantalla con contraseña, luego de 15 minutos de inactividad.
6.16 Todos los Equipos de trabajo del personal de ISP deben ser apagados una vez que los funcionarios terminen su jornada de trabajo.
6.17 Si los funcionarios tienen que dejar sus computadores personales encendidos y conectados a la red fuera de horario de oficina, estos equipos deben contar con sistemas de seguridad aprobados.
6.18 Las sesiones que se encuentren inactivas serán desconectadas después de un periodo de inactividad.
6.19 El acceso a información, puede ser otorgado de manera individual o ser otorgado a grupos de usuarios.
6.20 Las actividades que afectan información sensible de sistemas en producción, deben ser reconstruibles a partir de registros de transacciones.
6.21 Las herramientas de monitoreo u observación de actividades computacionales deben ser usadas con una notificación previa a los usuarios involucrados, a excepción de una investigación de actividades criminales.
6.22 Los mensajes enviados por el sistema electrónico de correos de la organización sólo pueden ser leídos bajo los requerimientos establecidos en la normativa legal, en caso de persecución criminal o administrativa.
6.23 Todos los dispositivos móviles como notebooks, Smartphones y PDAs entre otros, que contienen información sensible de la Organización, deben considerar protección o encriptación de disco duro y archivos.
6.24 Antes de otorgar los permisos de trabajo remoto a funcionarios de la organización, se debe firmar un acuerdo de confidencialidad que proteja la información sensible de la organización.

6.25 Los accesos a las salas de equipos de laboratorio y de análisis que requieran restricción de ingreso, serán de responsabilidad del encargado del área, ya sea, en la definición de quienes puedan ingresar y el control de acceso utilizado para ello.
6.26 Los accesos físicos y remotos de externos (proveedores, visitas u otros) deben ser controlados.

## 7. DIFUSIÓN

La política de seguridad, sus normas, procedimientos y estándares, y sus correspondientes actualizaciones y/o modificaciones, como también las resoluciones, oficios y/o circulares que emanen del FCPC de Jubilación y Cesantía de los Servidores de la Superintendencia de Bancos o del Encargado de Seguridad de la Información, se publicarán en el Banner del Sistema de Seguridad de la Información de la página de la intranet del Fondo. El Encargado de Seguridad de la Información será el responsable de gestionar con el administrador de la intranet las publicaciones correspondientes.

## 8. REVALUACIÓN

La política de seguridad, sus normas, procedimientos y estándares que se aplican a los activos de información serán examinados, revisados y reevaluados por el Comité de Seguridad cada dos (2) años y extraordinariamente cuando ocurra un incidente de seguridad que afecte a un activo de información catalogado con riesgo medio y/o alto, de manera de introducir las modificaciones apropiadas.

## 9. CUMPLIMIENTO

El cumplimiento de las políticas de seguridad, sus normas, procedimientos y estándares, deberá ser una tarea cotidiana y de estricta aplicación por parte de todos los funcionarios, desde el más alto nivel, hasta el último funcionario del escalafón. El incumplimiento de la presente política expone a quien la vulnere a las sanciones pertinentes según la resolución de las investigaciones regidas por vía legal o por un sumario según sea el caso.

Dado en la ciudad de Quito DM., el 16 de octubre de 2023.

**Ing. Jaime Julián Zambrano Borja,**
**PRESIDENTE DEL CONSEJO DE ADMINISTRACION DEL FCPC DE JUBILACIÓN Y CESANTÍA DE LOS SERVIDORES DE LA SUPERINTENDENCIA DE BANCOS**

**LO CERTIFICO, Quito, Distrito Metropolitano, el 19 de octubre de 2023**

| | | |
|---|---|---|
| **Elaborado por:** | Comité de Riesgos | Acta Nro.: FCPCJCSSB-CR-2023-005-A de 16 de octubre de 2023 |
| **Aprobado por:** | Consejo de Administración | Acta Nro.: FCPCJCSSB-CA-2023-008-A de 19 de octubre de 2023 |

## CONTROL DE REVISIONES

| Número de revisión | Fecha | Motivo | Aprobado por | Número de Acta y resolución |
|---|---|---|---|---|
| Versión 1.0 | Oct-2023 | Emisión | Comité de Riesgos | FCPCJSSB-CR-2023-004-A |
| Versión 2.0 | Oct-2023 | Emisión | Comité de Riesgos | FCPCJSSB-CR-2023-005-A |
| FINAL | Oct-2023 | Emisión | Consejo de Administración | FCPCJSSB-CA-2023-008-A |