INSTRUCTIVO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL FOSAFFI

FEBRERO DE 2013

INDICE

I. GENERALIDADES

A. Antecedentes

En la actualidad la información del FOSAFFI se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos del negocio se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Nuestra institución, los sistemas y red de información pueden enfrentar amenazas de seguridad que incluye entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con la promulgación del presente Instructivo del Sistema de Gestión de la Seguridad de la Información del FOSAFFI, se formaliza el compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

La elaboración del presente Instructivo del Sistema de Gestión de la Seguridad de la Información, toma de referencia metodológica aquellos conceptos de la norma UNE-ISO/IEC 17799 "Código de buenas prácticas para la Gestión de la Seguridad de la Información" considerando lo aplicable al FOSAFFI.

B. Base legal.

La elaboración del presente Instructivo del sistema de gestión de la seguridad de la información, está fundamentado en los artículos 56 al 60 de las Normas Técnicas de Control Interno Específicas del Fondo de Saneamiento y Fortalecimiento Financiero (FOSAFFI), autorizadas por decreto No 02 de la Corte de Cuentas de la República, publicado en el Diario Oficial No 84, Tomo 391, de fecha 5 de mayo de 2011.

C. Ámbito de aplicación.

El presente Instrumento es de aplicación general por todos los empleados y Funcionarios del FOSAFFI, terceros, contratistas, y usuarios que utilizan sus sistemas y servicios de información, para garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por todos los empleados del FOSAFFI o terceros de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

II. OBJETO.

Regular la información en el más amplio nivel de detalle a los usuarios, funcionarios y empleados del FOSAFFI, de las normas y mecanismos que deben cumplir y utilizar para salvaguardar los elementos tecnológicos de la red Institucional, así como la información que es procesada y almacenada en estos.

Fondo de Saneamiento y Fortalecimiento Financiero — PRESIDENCIA

III. DEFINICIONES.

Activo: En el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar los equipos informáticos o servicios, a través de terminales o equipos remotos, físicamente separados de la institución.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log: Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP's involucradas en el proceso, etc.)

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comité ejecutivo: Instancia de coordinación y comunicación interna del FOSAFFI, formada por los responsables de las distintas unidades organizacionales del FOSAFFI.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Cuenta: Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad: Los recursos de información sean accesibles, cuando estos sean necesitados.

Encriptación: Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

Integridad: Proteger la información de alteraciones no autorizadas por la organización.

Impacto: Consecuencia de la materialización de una amenaza.

ISO: (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.

IEC: (Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.

Normativa de Seguridad ISO/IEC 17799: (Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a la institución.

Responsabilidad: En términos de seguridad, significa determinar que individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.

Seguridad de la Información: La información se considera un activo esencial para el cumplimiento de la misión de la Institución, por lo tanto necesita ser protegido adecuadamente. La información puede existir en muchas formas, cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida. (Impresa, almacenada electrónicamente, transmitida utilizando medios electrónicos, mostrada en películas o contenida en una conversación).La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del FOSAFFI en el cumplimiento de su misión mediante la ejecución de sus procesos críticos y el cumplimiento de las disposiciones legales que lo regulan. Se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. El alcance de la política de seguridad de la información son todos los empleados, terceras personas, contratistas y usuarios del FOSAFFI que utilizan sus sistemas y servicios de información.

Servicio: Conjunto de aplicativos o programas informáticos, que apoyan la labor educativa, académica y administrativa, sobre los procesos diarios que demanden información o comunicación de la institución.

SGSI: Sistema de Gestión de Seguridad de la Información

Soporte Técnico: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la Institución.

Riesgo: Posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

Terceros: Entes fiscalizadores, Instituciones como Dirección de protección al consumidor, proveedores, clientes.

Usuario: Definase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación académica o laboral con la institución.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo

IV. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

A. Organización de la Seguridad de la Información.

1. El compromiso de la Institución con la seguridad de la información se establece elevando la toma de decisiones sobre este tema al Comité Administrador del FOSAFFI, autoridad máxima.

2. La coordinación y la asignación de responsabilidades de la seguridad de la información estarán contenidas dentro de la descripción del puesto Jefe de la Sección Informática.

Fondo de Saneamiento y Fortalecimiento Financiero — PRESIDENCIA

3. Las revisiones de la seguridad de la información forman parte del alcance de las visitas de Entes de Control Interno y Externos de la Institución (Auditoría Interna, Auditoría Externa, Superintendencia del Sistema Financiero, y Corte de Cuentas de la República entre otros).

4. El FOSAFFI protegerá su información confidencial o sensible mediante los acuerdos de confidencialidad o no-divulgación, siendo los responsables de esta información quienes gestionarán ante el coordinador de la seguridad de la información la elaboración e implementación de estos acuerdos.

B. Seguridad del personal.

1. El acceso a la información de la Institución otorgada a un empleado o tercero no otorga ningún derecho sobre la misma y su uso está limitado para el fin proporcionado.

2. La información que maneja o manipula un empleado, no puede ser divulgada a terceros o fuera del ámbito de laboral.

3. Los empleados son responsables de las acciones causadas por sus operaciones con su usuario y el equipo de la red institucional.

4. Todos los empleados permanentes o temporales, terceras personas, contratistas que laboran para el FOSAFFI tendrán acceso sólo a la información pertinente para el desarrollo de sus actividades. En el caso de personas ajenas al FOSAFFI que necesiten tener acceso a información, se deberá solicitar por escrito a la Gerencia General la respectiva autorización sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

5. Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como confidencial y/o crítica.

6. El sistema de correo electrónico y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada empleado y de las actividades contratadas en el caso de los contratistas y pasantes.

7. La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en FOSAFFI o en sitios de trabajo alternos, es propiedad exclusiva de la entidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

8. En cualquier momento que un empleado publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la entidad.

C. Gestión de activos.

1. Los jefes de las distintas unidades organizativas del Fondo son los responsables de los activos asignados a su unidad para el cumplimiento de los objetivos, llámese activos los relacionados a tecnología tales como: hardware, software, aplicaciones o información.

2. Los jefes de las distintas unidades organizativas del Fondo deberán proponer a la Gerencia General la clasificación de la información que produzca o genere cada uno de sus unidades organizativas del Fondo. Esta clasificación consistirá en definir si esta es información: pública, si es de carácter confidencial o de uso exclusivo de la unidad organizativa del Fondo que lo produce.

D. Seguridad física y de entorno.

1. El usuario deberá mantener su puesto de trabajo limpio. Asimismo, es responsable de los daños ocasionados a su equipo si no guarda las precauciones necesarias en el manejo de objetos tales como grapas o clips, o por el derramamiento de bebidas o comidas que se pueden caer accidentalmente dentro del equipo

2. Deberá existir un área específica para los servidores institucionales, dotado con las medidas de seguridad siguientes: acceso restringido, paredes sólidas, aire acondicionado, alimentación eléctrica ininterrumpida, detector de humo, detector de incremento de temperatura y extintor de incendios.

3. Ningún empleado está autorizado para trasladar equipos fuera de su área originalmente asignada.

4. Los jefes de las distintas unidades organizativas del Fondo son los que autorizan el traslado o movimientos de equipos, archivos o sistemas de información.

5. Todo traslado de equipos deberá notificarse al Departamento Administrativo Financiero para su actualización en los controles respectivos.

6. Ningún usuario está autorizado para efectuar cambios, modificaciones o reparaciones de hardware en sus computadoras. Los únicos autorizados son el personal técnico de la Sección de Informática

7. El personal técnico de la Sección de Informática verificará que los equipos informáticos estén conectados a tomas de energía regulada y con respaldo de batería (UPS). No estará permitido conectar los equipos a otras fuentes de energía eléctrica que no se encuentran debidamente protegidas. Asimismo, no deberán conectarse otros aparatos eléctricos (radios, máquinas de escribir, calculadoras, etc.) en el mismo toma del computador.

8. Durante el mantenimiento a las computadoras un técnico de la Sección de Informática debe estar presente para vigilar que el personal de mantenimiento no intervenga en la seguridad de sus archivos.

9. Si el equipo tiene que ser llevado fuera de la institución, deberá existir un documento donde se justifique el alcance, resultados, tiempo y nombre de la persona responsable del equipo. También deberá registrarse el acuse de recibido, fechas de salida y entrada.

10. Todos los computadores portátiles se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la oficina de informática.

Fondo de Saneamiento y Fortalecimiento Financiero PRESIDENCIA

E. Administración de comunicaciones y operaciones.

1. Todos los equipos como servidores, PC, portátiles, router, switch deberán tener claves para su acceso y/o modificación de su configuración.

2. La Sección de Informática deberá llevar registro de cambios a las configuraciones de estos equipos.

3. La Sección de Informática deberá llevar registro de incidentes relacionados con la operatividad normal de las distintas unidades organizativas del Fondo.

4. Las direcciones de red internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Institución, deberán ser considerados y tratados como información confidencial.

5. Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Institución, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

F. Control de acceso.

1. Todo usuario de la red tendrá un código y una clave de acceso, que serán asignados inicialmente por el Administrador de la red durante la creación del usuario en el sistema y será facilitada exclusivamente al usuario. El código de clave será el mismo código de empleado, en el caso de terceras personas o contratista será un código temporal con el prefijo UT. El usuario asume la responsabilidad de conservar en secreto su clave. Se controlará que la clave sea fuerte, el cambio no exceda los tres veces, los intentos fallidos de conexión.

2. Todas las operaciones que realizan los usuarios en la red quedan registradas en los servidores. Cada uno de los usuarios es responsable de las operaciones registradas con su código de acceso. Los usuarios de la red tendrán derecho a una sola sesión. No se permitirán las sesiones múltiples.

3. El Gerente y Jefes autorizarán la creación de usuarios de red y de los sistemas, indicando los roles y permisos atendiendo el procedimiento correspondiente.

4. Las cuentas de usuario son estrictamente personales por lo que deberá conservar la clave en secreto, todo registro realizado en los sistemas con su código asignado será considerado de su completa responsabilidad. Cuando sepa o sospeche que su clave es del conocimiento de una tercera persona, deberá solicitar de inmediato el cambio de clave.

G. Sistemas de Información.

1. La seguridad será parte integral para los sistemas de información de la Institución, por lo que los requerimientos de seguridad se deberán identificar, justificar y acordar en la fase de requerimientos del proyecto, antes del desarrollo y/o implementación de los sistemas de información.

2. La prevención de errores, la pérdida o modificación de no autorizada o mal uso de la información en los sistemas de información se basará en el diseño de controles (entrada de

datos, procesamiento interno, salida de datos) que aseguren el procesamiento correcto del aplicativo, así como la autenticidad y protección de la integridad de los mensajes.

3. La protección de los datos sensibles se realizará mediante la aplicación de técnicas de encriptamiento proveídas por la infraestructura tecnológica disponible en la Institución.

4. Deberá mantenerse controlado y protegido la instalación del software operacional, la selección de los datos proporcionado para pruebas, el código fuente de los programas, y los ambientes tecnológicos de desarrollo y soporte.

5. La Institución realizará al menos una vez al año el análisis de vulnerabilidad de su infraestructura tecnológica para fortalecer la gestión de los riesgos tecnológicos.

6. Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración y operación y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

7. Toda solicitud de cambios en programas y datos de producción, deberá ser suscrita y debidamente justificada por el Jefe de la unidad organizativa del Fondo usuario del sistema y el Gerente General; en tal sentido dichos funcionarios compartirán de manera solidaria las responsabilidades que derivan de la decisión. Esta solicitud deberá ser enviada a la Sección de Informática para que emita su opinión respecto a la viabilidad técnica de lo solicitado.

8. Para las aplicaciones que son compartidas por dos o más unidades organizativas del Fondo, la incorporación del cambio será con el visto bueno y la responsabilidad de ambas unidades y la autorización la dará el Gerente General, quien también será responsable.

H. Gestión de incidentes de seguridad de la información

El establecimiento de la presente política para el reporte de eventos y debilidades de la seguridad de la información concerniente con los sistemas y servicios de información permite que se realice una acción correctiva oportuna.

1. Los eventos o debilidades de la seguridad de la información deberán ser reportados por las Jefaturas o Gerentes al Jefe de la Sección de Informática por medio del sistema HELP DESK tan pronto como sea posible.

2. Todos los empleados, terceras personas, o contratista, deberán informar tan pronto como sea posible a sus Jefes o Gerente, cualquier debilidad de seguridad de la información observada o sospechada.

3. El Jefe de la Sección de Informática deberá asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información reportados. Una vez resuelto el incidente se deberá evaluar y documentar la solución dada en el sistema HELP DESK para que forme parte del conocimiento de la Institución sobre este tema.

I. Continuidad de las operaciones.

La continuidad de los procesos críticos ante una catástrofe o falla importante en los sistemas de información minimiza el impacto sobre la organización y recupera de las pérdidas de activos de información hasta un nivel aceptable a través de una combinación de controles preventivos y de

recuperación. Los recursos de continuidad están identificados previamente incluyen las operaciones, el personal, los materiales, el transporte y los medios.

1. El Comité de Auditoría conocerá anualmente el resultado de la revisión y prueba del plan de continuidad del sistema informático y la correspondiente evaluación de riesgos, para garantizar que se mantiene marco único con el plan de continuidad del negocio.

2. La estrategia del plan de continuidad del sistema informático para la Institución es la implementación de un centro de datos alterno ubicado fuera de la ciudad sede de las oficinas centrales de la Institución. La documentación de los procesos críticos y los archivos de datos de los usuarios forman parte de los respaldos de información de la Institución.

V. RESPONSABILIDADES

A. Cumplimiento.

La Institución está comprometida con el cumplimiento a cualquier ley; regulación estatutaria, reguladora o contractual; normativa de los entes de control interno; y cualquier requerimiento de seguridad de la información en el diseño, operación, uso y gestión de los sistemas de información.

1. El Jefe de la Sección de Informática incluirá con la divulgación del presente Sistema de Gestión de Seguridad de la Información la identificación de la Legislación o Normativa aplicable de estricto cumplimiento con el apoyo del Departamento Jurídico de la Institución.

2. El Jefe de la Sección de Informática incluirá con la divulgación del presente Sistema de Gestión de Seguridad de la Información la Ley de la Propiedad Intelectual y la Ley de Acceso a la Información Pública.

3. La protección de los registros de la Institución se fundamenta en lo estipulado por la Ley de Acceso a la Información Pública.

4. Todos los funcionarios y empleados deberán hacer uso racional de los equipos y servicios informáticos proporcionados para el cumplimiento de sus actividades, exclusivamente para fines institucionales.

5. Cuando un miembro del personal dejare de laborar para la Institución, el jefe de la unidad organizativa del Fondo correspondiente en coordinación con la Sección de Informática, deberán de corroborar los bienes informáticos que entregan, incluyendo archivos de información Institucional, levantando el acta correspondiente.

6. Cuando se identifica una actividad no autorizada por parte de un usuario, esta actividad será puesta en atención del gerente o jefe a cargo para que considere la acción disciplinaria y/o legal apropiada.

7. El Gerente y Jefes deberán revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas y estándares de seguridad contenidos en el presente documento como y cualquier otro requerimiento legal de seguridad.

8. El Departamento de Auditoría Interna en el cumplimiento de su plan mantendrá controles para salvaguardar las herramientas de auditoría, para evitar cualquier mal uso o trasgresión posible,

debiendo estar separadas en un ambiente tecnológico independiente del ambiente tecnológico de operación y de desarrollo.

B. Obligaciones

1. El Jefe de la Sección de Informática deberá:

   a) Desarrollar, revisar, y publicar el presente instructivo.

   b) Supervisar la seguridad de los sistemas y equipos

   c) Vigilar el cumplimiento de este instructivo.

   d) Divulgar el contenido del instructivo por lo menos una vez al año, y de sus modificaciones inmediatamente que sean aprobadas.

   e) Brindar capacitación en materia de seguridad informática a los usuarios del Fondo, con el fin de concientizar la importancia de acatar las medidas de seguridad.

2. El Comité Administrador será responsable de autorizar el presente Instructivo.

3. La Auditoría Interna será responsable de incluir en su plan de trabajo la evaluación y aplicación del presente instructivo.

C. Prohibiciones.

1. No se permitirá compartir la información del disco de las computadoras entre los usuarios de la red.

2. Los usuarios no deberán enviar mensajes de contenido indebido o mensajes que violen la ética de la Institución.

3. Se prohíbe a los usuarios enviar mensajes estilo cadena o propaganda postal a través del sistema de correo electrónico.

4. No es permitido el uso del software no autorizado. Esto incluye también todo tipo de software de oficina que no forme parte del estándar autorizado.

5. Se prohíbe hacer uso del software fuera de las instalaciones del FOSAFFI.

6. Los impresores no deberán ser utilizados como dispositivos de emisión de copias, únicamente de documentos originales.

7. Se prohíbe a los usuarios el descargar archivos de Internet tales como juegos, protectores de pantallas y música.

8. Los usuarios no deberán alterar la configuración del computador asignado, los técnicos de informática son los únicos autorizados para modificar las distintas configuraciones tales como software instalado, correo externo, correo interno, Internet, etc.

Fondo de Saneamiento y Fortalecimiento Financiero PRESIDENCIA

9. Se prohíbe acceder a los sistemas de información para realizar actualizaciones indebidas o fraudulentas, utilizando usuarios y claves propios o de otros usuarios, esto se considerará como falta grave.

10. Dejar encendido el equipo después de terminadas las labores.

11. Comer o tener recipientes con líquidos junto a los equipos de computación.

12. Instalar juegos en la computadora.

13. Proporcionar a terceros su cuenta y clave de acceso.

14. Deshabilitar el Antivirus.

VI. DISPOSICIONES ESPECIALES

1. La Gerencia General del Fondo velará porque se le dé estricto cumplimiento al presente instructivo; las situaciones no contempladas serán resueltas por el Comité Administrador del Fondo

2. La Gerencia General del Fondo emitirá los procedimientos e instrucciones necearías para el cumplimiento de lo dispuesto en este instructivo.

3. El presente instructivo será implementado por la Sección de Informática.

VII. VIGENCIA, PUBLICACION, DISTRIBUCION Y DIVULGACION

1. El presente instructivo entrará en vigencia ocho días después de su aprobación.

2. Con la entrada en vigencia del presente instructivo, quedará sin efecto el Plan de contingencia informática y de continuidad de operaciones, aprobado por la Presidencia del FOSAFFI de fecha 26 de septiembre de 2008; y el Instructivo de Administración y Optimización de los Recursos Informáticos, aprobado por el Comité Administrador en la CA 08/2009 de marzo de 2009.

3. La Gerencia General conservará un original de este instructivo y entregará una copia controlada, la cual quedará en poder de la Sección de Control y Seguimiento.

4. La Sección de Informática realizará la divulgación de este instructivo, utilizando la intranet institucional y otras formas, con el apoyo de la Sección de Control y Seguimiento

VIII. CUADRO DE CONTROL DE MODIFICACIONES

CUADRO DE CONTROL DE MODIFICACIONES

Nº Revisión	Versión Anterior	Versión Aprobada	Aprobador y fecha