MINISTERIO DE AGRICULTURA Y GANADERÍA
SERVICIO FITOSANITARIO DEL ESTADO (SFE)

- **Informe de Cumplimiento y Control Interno de Tecnologías de Información, noviembre del 2009**

Ing. Fabián Cordero
Auditor de T.I.

TABLA DE CONTENIDOS

Contenido

RESUMEN EJECUTIVO

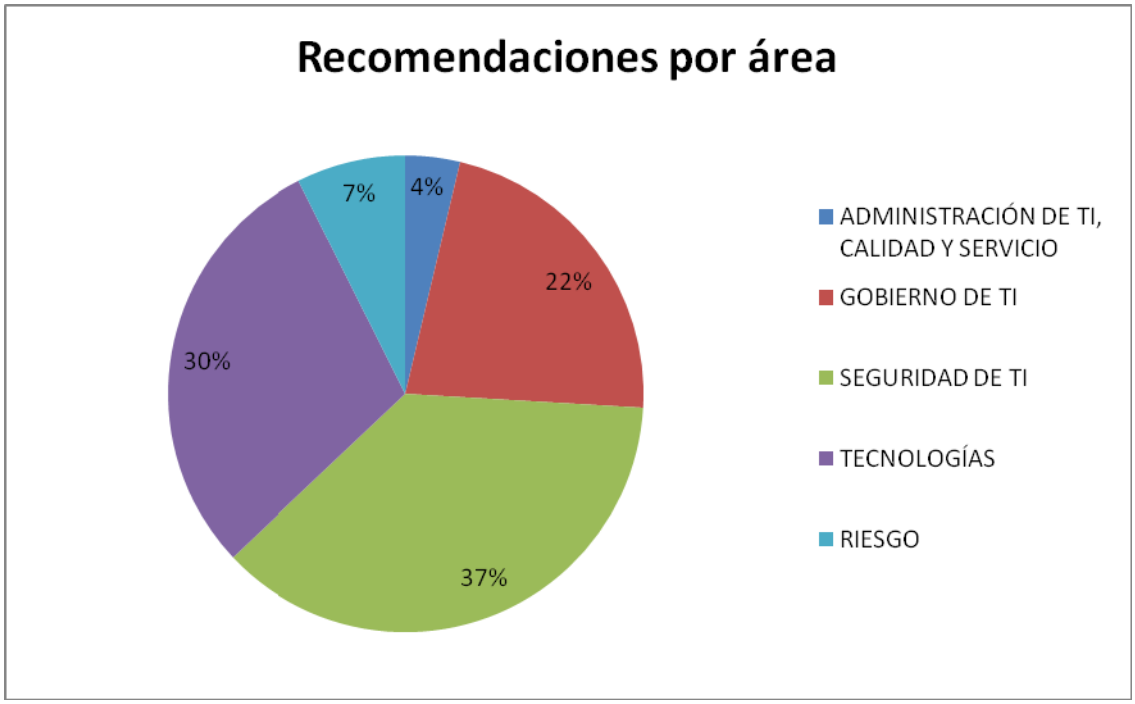
PROPÓSITO Y LIMITACIONES

El resumen ejecutivo está destinado para proporcionar el punto de vista de la auditoría, y destacar en un resumen básico, los hallazgos significativos discutidos en el informe detallado de auditoría. Se debe tener el cuidado de llegar a conclusiones basadas solamente en una revisión o una lectura de este resumen.

Es necesario leer las secciones específicas del detalle y/o el informe en su totalidad para obtener el conocimiento de los antecedentes, repercusiones, y recomendaciones referente a cada resultado y/o hallazgo.

ESTADÍSTICAS DE LA EJECUCIÓN DEL PROGRAMA DE TRABAJO

Como resultado de la evaluación del sistema de control interno informático del SFE, se identificaron 27 oportunidades de mejora (recomendaciones) que pueden ser clasificadas en 5 áreas (agrupación de hallazgos considerando su naturaleza) que se describen a continuación:

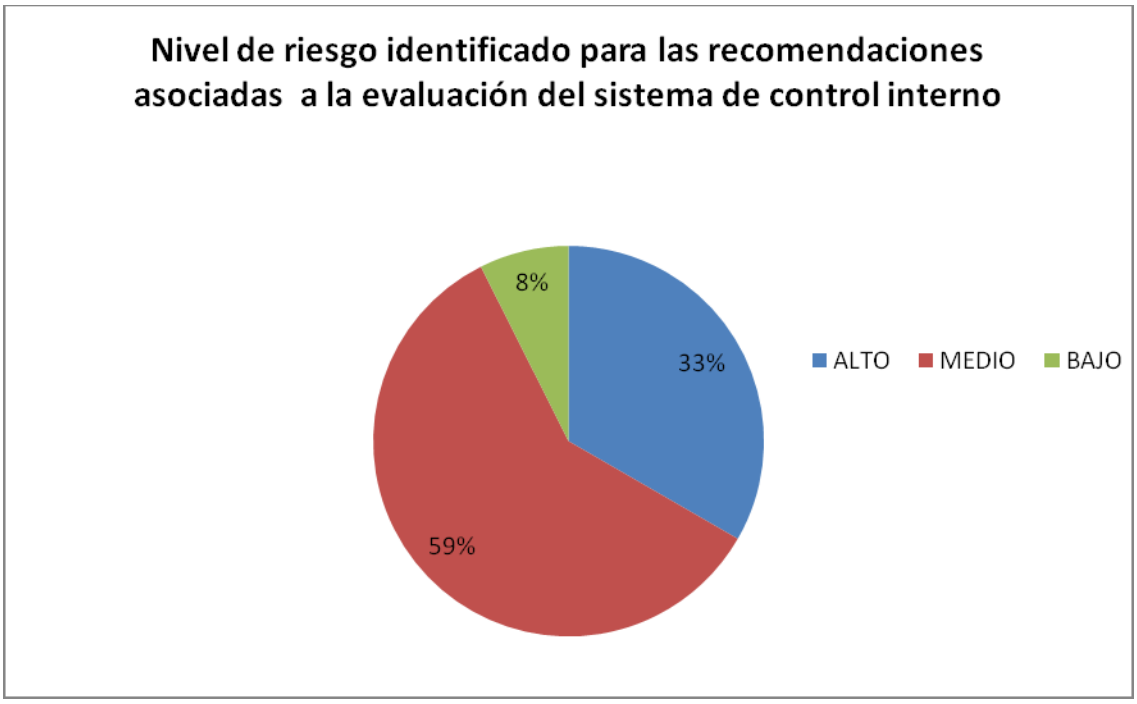


Recomendaciones

AREA	*CANTIDAD*
ADMINISTRACIÓN DE TI, CALIDAD Y SERVICIO	1
GOBIERNO DE TI	6
SEGURIDAD DE TI	10
TECNOLOGÍAS	8
RIESGO	2

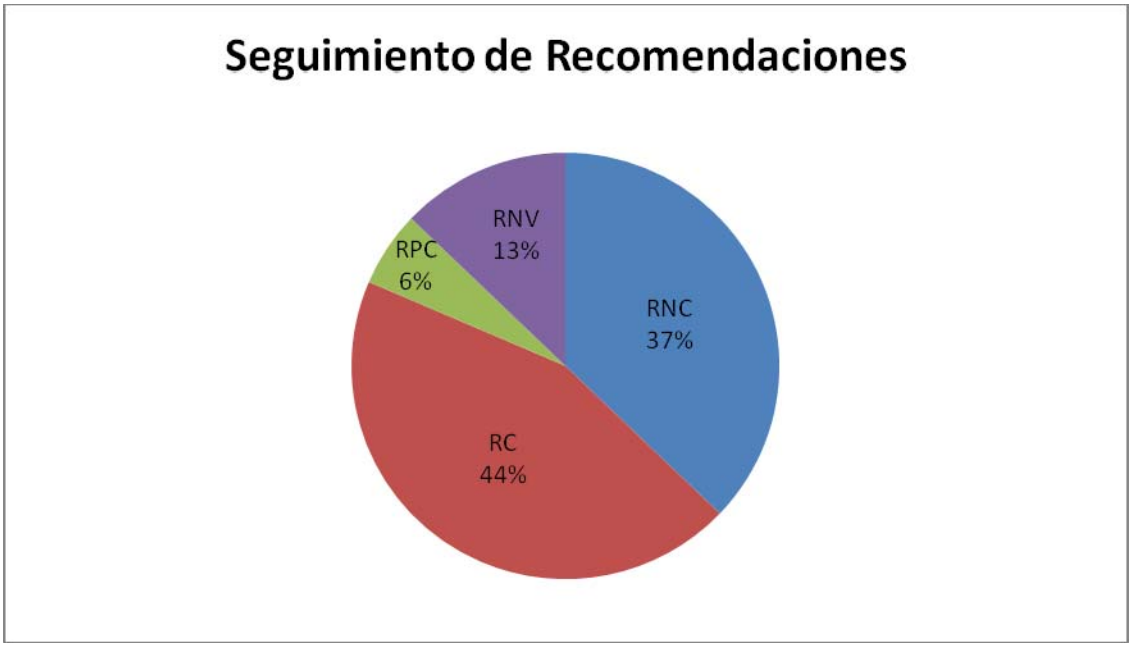
Además, como resultado de la evaluación realizada se clasificaron las 27 oportunidades de mejora en tres categorías de riesgo, según se muestra en la tabla siguiente:

CATEGORIA DE RIESGO	*CANTIDAD*
RIESGO ALTO	9
RIESGO MEDIO	16
RIESGO BAJO	2



Asimismo, se le dio seguimiento a las recomendaciones contenidas en el informe de auditoría, comunicado por la Auditoría Interna del MAG a la administración activa mediante oficio AI 307-2003 del 19/12/2003, en el cual se identificaron 70 oportunidades de mejora, cuyo estado se detalla a continuación:

ESTADO	*CANTIDAD*
Recomendaciones No Cumplidas (RNC)	26
Recomendaciones Cumplidas (RC)	32
Recomendaciones en Proceso de Cumplimiento (RPC)	4
Recomendaciones No Vigentes (RNV)	10



HALLAZGOS

1. DEBILIDADES EN LA ADMINISTRACIÓN DE TI, CALIDAD Y SERVICIOS.

1.1 OBSERVACIÓN 1: NO SE CUENTA CON UNA METODOLOGÍA PARA LA GESTIÓN DE LA CALIDAD

CONDICIÓN:

Actualmente la Sección de Informática del SFE no cuenta con una metodología para la gestión de la calidad en procesos informáticos.

Se determinó que dicha Sección para comprobar la calidad y el buen funcionamiento de los sistemas y procesos en general, basa su gestión únicamente en pruebas satisfactorias y en la información de los contratos.

2. DEBILIDADES VINCULADAS CON EL GOBIERNO DE T.I.

2.1 OBSERVACIÓN 1: NO SE CUENTA CON UNA POLÍTICA ORGANIZACIONAL PARA CONCENTRAR LA FUNCIÓN DE ADQUISICIÓN Y ADMINISTRACIÓN DE TECNOLÓGICA EN LA SECCIÓN DE INFORMÁTICA DEL SFE.

CONDICIÓN:

Actualmente el SFE no cuenta con una política documentada y aprobada sobre la centralización de la adquisición y administración de la plataforma tecnológica.

2.2 OBSERVACIÓN 2: POCA EJECUTORÍA ACTIVA DE LA COMISIÓN INFORMÁTICA.

CONDICIÓN:

De acuerdo con la revisión realizada a la estructura organizacional para la administración de los recursos informáticos, se observó que el SFE cuenta con una Comisión para la gestión informática. Sin embargo, esta Comisión solo se ha reunido una vez en el presente año, con el fin de comparar las compras de equipo solicitadas por los diferentes departamentos con los inventarios actualizados del equipo de cómputo que posee la Sección de Informática.

2.3 OBSERVACIÓN 3: NO SE CUENTA CON UN PLAN ESTRATÉGICO A LARGO PLAZO PARA LA SECCIÓN DE INFORMÁTICA DEL SFE.

CONDICIÓN:

Al efectuar la revisión de la administración y planificación de los recursos informáticos del SFE, se determinó que aún no se ha elaborado un plan estratégico a largo plazo de tecnologías de información. Actualmente el SFE solamente cuenta es con un Plan Operativo Institucional (POI).

2.4 OBSERVACIÓN 4: SE CARECE DE UN MANUAL DE FUNCIONES PARA LA SECCIÓN DE INFORMÁTICA DEL SFE.

CONDICIÓN:

Al efectuar la revisión sobre las cargas de trabajo de los colaboradores de la Sección de Informática, se determinó que no existe un manual de funciones para cada unos de los cargos establecidos en dicha Sección. Actualmente el SFE, únicamente cuenta con el "Manual de Clases Anchas" de la Dirección General de Servicio Civil.

2.5 OBSERVACIÓN 5: INADECUADA SEGREGACIÓN DE FUNCIONES PARA EL ENCARGADO DE ADMINISTRAR LAS BASES DE DATOS DEL SFE.

CONDICIÓN:

Al efectuar el estudio sobre las funciones realizadas por el personal de la Sección de Informática, se determinó que el encargado de administrar las bases de datos del SFE, además realiza funciones de desarrollador de sistemas.

2.6 OBSERVACIÓN 6: NO SE CUENTA CON UNA BASE DE DATOS DE CONOCIMIENTO PARA EL AREA DE TI.

CONDICIÓN:

El SFE no ha implementado una base de datos que le posibilite registrar el conocimiento y la resolución de problemas específicos relacionados con las tecnologías de información. Esta base podría informar y orientar sobre la forma de utilizar dichas tecnologías a nivel organizacional, unificando los criterios de desempeño y cursos de acción que deberán seguirse para cumplir con los objetivos planteados; además de poder agrupar el conocimiento de las diferentes áreas usuarias del SFE.

3. DEBILIDADES EN LA SEGURIDAD DE T.I.

3.1 OBSERVACIÓN 1: NO SE TIENE LA PRÁCTICA DE COMUNICAR EN FORMA PERIODICA Y CONSTANTE CAMBIOS DE PERSONAL EN EL SFE A LA SECCIÓN DE INFORMÁTICA.

CONDICIÓN:

Actualmente no se cuenta a nivel organizacional con una política en donde se defina que la Sección de Recursos Humanos del SFE debe suministrar periódicamente a la Sección de Informática un listado de las personas que han sufrido alguna rotación en los distintos puestos del SFE (renuncias, despidos o vacaciones prolongadas, etc), con el fin de realizar los respectivos cambios de roles y privilegios en los sistemas de información y la red.

3.2 OBSERVACIÓN 2: EL ÁREA EN DONDE SE ENCUENTRAN LOS SERVIDORES DEL SFE NO CUENTA CON UNA ADECUADA SEGURIDAD.

CONDICIÓN:

Al efectuar la revisión del área en donde se encuentran los servidores del SFE, se determinó que no existen detectores de humo, ni alarmas contra incendio, tampoco se cuenta con cámaras de vigilancia ni un deshumidificador. Es conveniente la instalación de este último dispositivo en el cuarto de servidores, ya que la humedad puede ocasionar la corrosión de los componentes internos y la degradación de propiedades tales como la resistencia eléctrica, la conductividad térmica, la resistencia física y el tamaño[1]. Además, no es conveniente que los servidores del Servicio Nacional de Salud Animal (SENASA) y la "Central Telefónica" se encuentre en el área de servidores del SFE, por cuanto entran personas ajenas a la Sección de Informática del SFE, poniendo en riesgo la información almacenada en esos servidores. Por otra parte es recomendable la instalación de un control de acceso biométrico[2] al cuarto de servidores.

[1] Se refiera a la masa molecular del computador.

[2] La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.
Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica

3.3 OBSERVACIÓN 3: FALTA DOCUMENTAR EL PROCEDIMIENTO PARA DEFINIR PERFILES, ROLES Y NIVELES DE PRIVILEGIO A LOS USUARIOS DE LOS SISTEMAS IMPLANTADOS EN EL SFE.

CONDICIÓN:

Al efectuar la revisión de los perfiles, roles y niveles de privilegio de los usuarios de los sistemas implantados en el SFE, se determinó que actualmente ni la Sección de Informática ni las demás Unidades usuarias del SFE, cuentan con un procedimiento debidamente documentado para definir este tipo de perfiles.

3.4 OBSERVACIÓN 4: AUSENCIA DE SEGURIDAD EN EL SISTEMA DE PLANILLAS DEL SFE.

CONDICIÓN:

Al realizar la valoración a los sistemas de información implantados en el SFE, se determinó que el sistema de planillas esta desarrollado en FOX (lenguaje de programación que nació varias décadas atrás). Además, dicho sistema no presenta una seguridad adecuada debido a las siguientes razones:

- El sistema es portable, es decir se guarda en cualquier medio de almacenamiento externo, permitiendo instalar la aplicación en cualquier terminal.
- El sistema no solicita el cambio de clave automáticamente ni se desactiva en caso de no ser utilizado después de cierto periodo de tiempo.
- El sistema lo manipulan dos personas, las cuales cuentan con el mismo usuario y misma contraseña.
- El sistema genera archivos dbf (Base de datos), que se guardan en la máquina del usuario.
- No presenta bitácoras para verificar alguna inadecuada manipulación de la información.
- No se lleva un registro histórico de las claves.
- No existe un procedimiento automatizado o administrativo para la detección de accesos no autorizados.
- No se llevan los tiempos ni días de acceso por terminal.

Por otra parte el sistema presenta algunas limitaciones como:

- No desactiva a los empleados interinos, es decir, el encargado de la planilla debe estar revisando constantemente cuando una persona interina ya no labora para el SFE, de lo contrario la planilla de pagos se genera con esas personas.
- No calcula liquidaciones.
- No cuenta con filtros para reportes históricos.
- No presenta la posibilidad de calcular anualidades.
- No se posee el código del sistema, lo que se conoce en informática como una caja negra.
- Se depende 100% del mantenimiento por parte del proveedor.

Cabe mencionar que el Sistema de Planillas es utilizado además por el SENASA, aún cuando el propietario del sistema es el SFE; y el mantenimiento al mismo es cubierto con recursos del SFE y del SENASA. Dicha situación eventualmente podría estar generando un incumplimiento a la Ley de Protección Fitosanitaria N° 7664, por cuanto el SFE tiene la imposibilidad de compartir recursos con órganos que no estén vinculados con el cumplimiento de sus objetivos.

3.5 OBSERVACIÓN 5: IDENTIFICACIÓN DE USUARIOS GENÉRICOS EN LA PLATAFORMA TECNOLÓGICA

CONDICIÓN:

Al realizar un estudio sobre los usuarios que se encuentran definidos en la plataforma tecnológica se identificó la existencia de usuarios genéricos como por ejemplo:

- Administrador Sitio Web.
- Aeropuerto.
- Cuarentena aeropuerto Daniel Oduber.
- Cuarentena Aeropuerto Tobias Bolaños.
- Cuarente Los Chiles.
- Dirección.
- Estación Cuarentena (Aeropuerto, Caldera, Golfito, Limón, Paso Canoas, Sixaola, Ventanilla Única).
- Fitosanitario (Caldera, de exportación, Limón).

- GSI.
- GTEUser.
- Laboratorio Laboratorio control calidad.
- Plaguicidas SFE.
- Prensa SFE.
- Recursos Humanos.
- Región (Brunca, Cartago, Chorotega, Esparza, Grecia, Guápiles, Huetar Norte, Puriscal)
- SICOIN.
- SICOININSTALLERUSER.
- SQL Admin.

Lo anterior provoca que en una misma terminal varios funcionarios puedan acceder a los sistemas de información con un mismo usuario, lo cual podría dificultar la determinación del responsable ante un posible mal manejo de la información.

3.6 OBSERVACIÓN 6: NO EXISTE UN PLAN DE CONTINGENCIAS INTEGRAL QUE AYUDE A SALVAGUARDAR LOS RECURSOS INFORMÁTICOS DEL SFE, ASÍ COMO GARANTIZAR LA CONTINUIDAD DE LAS OPERACIONES.

CONDICIÓN:

Según el análisis realizado a la continuidad de las operaciones, se determinó que la Sección de Informática del SFE, no cuenta con un plan de contingencias integral que en caso de imprevistos, permita la administración y utilización de los recursos tecnológicos de manera apropiada.

3.7 OBSERVACIÓN 7: NO EXISTE UN MECANISMO DE REPLICACIÓN AUTOMÁTICA EXTERNO PARA LOS SERVIDORES PRINCIPALES DEL SFE.

CONDICIÓN:

Al efectuar la revisión de los respaldos de la información almacenada en los servidores del SFE, se determinó que no se cuenta con un mecanismo de replicación automática en un lugar externo a las instalaciones del SFE. Dicha situación no estaría permitiendo garantizar la continuidad de las operaciones en forma inmediata en caso de falla del servidor principal localizado en oficinas centrales del SFE ubicadas en el Barreal de Heredia.

3.8 OBSERVACIÓN 8: POCO ESPACIO FÍSICO PARA LA SECCIÓN DE INFORMÁTICA.

CONDICIÓN:

El espacio físico con que cuenta la Sección de Informática del SFE es insuficiente para albergar adecuadamente la cantidad de recurso humano y equipo técnico. No obstante, el SFE tiene prevista la asignación de mayor espacio físico para la citada Sección, en el edificio que se está remodelando; situación que según la jefatura de esa área estaría mejorando las condiciones existentes.

3.9 OBSERVACIÓN 9: NO SE CUENTA CON UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN).

CONDICIÓN:

Al efectuar la revisión de la seguridad para el área de T.I. del SFE, se determinó que no existe un estudio de penetración contratado a una empresa especializada en ese tipo de consultarías, el cual podría mostrar ciertas debilidades en el área de telecomunicaciones.

3.10 OBSERVACIÓN 10: NO SE RESPALDA LA INFORMACIÓN CRÍTICA DE USUARIOS FINALES.

CONDICIÓN:

Actualmente las áreas usuarias llevan el control de varios procesos en hojas electrónicas o documentos de Word; sin embargo, esta información sólo se respalda en las máquinas de los usuarios.

4. DEBILIDADES EN TECNOLOGÍAS

4.1 OBSERVACIÓN 1: NO SE CUENTA CON UNA HERRAMIENTA AUTOMATIZADA PARA EL CONTROL DE VERSIONES

CONDICIÓN:

Al efectuar la revisión de la implementación de software, se determinó que el área de Análisis y Diseño de Sistemas no cuenta con una herramienta automatizada para controlar las versiones de las distintas aplicaciones en desarrollo.

4.2 OBSERVACIÓN 2: NO SE CUENTA CON PLANES DE PRUEBAS PARA LOS RESPALDOS DE LA INFORMACIÓN.

CONDICIÓN:

La Sección de Informática cuenta actualmente con un procedimiento para el respaldo de la información almacenada en los servidores; sin embargo, no se establecen los lineamientos necesarios para poder determinar la integridad de los datos almacenados.

4.3 OBSERVACIÓN 3: FALTANTE DE LICENCIAS DE SOFTWARE.

CONDICIÓN:

Al efectuar la revisión sobre la implementación de software, se determinó que el SFE tiene un déficit de licencias en algunos de los programas actualmente instalados.

4.4 OBSERVACIÓN 4: NO ESTA DOCUMENTADA LA METODOLOGÍA PARA LA ADMINISTRACIÓN DE PROYECTOS INFORMÁTICOS.

CONDICIÓN:

No se ha documentado el marco para el control de proyectos de TI, que contemple metodologías, planes, procesos de administración de riesgos, aseguramiento de la calidad entre otros aspectos que involucran la eficiente administración de proyectos tecnológicos.

4.5 OBSERVACIÓN 5: NO SE CUENTA CON UNA METODOLOGÍA PARA EL DESARROLLO DE SISTEMAS.

CONDICIÓN:

Se determinó que la Sección de Informática del SFE no cuenta actualmente con una metodología formal para el desarrollo de sistemas y mantenimiento de sistemas de información, la cual asegure el éxito y calidad de los proyectos a desarrollar.

4.6 OBSERVACIÓN 6: CARENCIA DE ESTUDIOS DE FACTIBILIDAD PARA PROYECTOS TECNOLÓGICOS.

CONDICIÓN:

Al efectuar la revisión de la "Gestión de Recursos Informáticos", se determinó al momento de realizar nuestra visita la ausencia de documentos en donde se notara un estudio de factibilidad de los diversos proyectos tecnológicos a desarrollar o desarrollados por la Sección de Informática del SFE.

4.7 OBSERVACIÓN 7: IMCUMPLIMIENTO DE LOS ESTÁNDARES DEFINIDOS PARA LA ADMINISTRACIÓN DE BASES DE DATOS.

CONDICIÓN:

Al efectuar la revisión de la documentación de los estándares que deben estar implantados en las "Bases de Datos" (DB) del SFE, se determinó que los mismos no se están cumpliendo. El estándar de BD menciona:

> *"…Siempre deberá existir un análisis de la base de datos antes de la implantación de cualquier Base de Datos o sus partes constituyentes y deberá contar, tanto en forma impresa como electrónica, al menos con los siguientes elementos:*
>
> *1º. Diagrama de Clases.*
>
> *2º. Diagrama entidad relación, con todas las tablas, llaves y las relaciones correspondientes.*
>
> *3º. Para cada procedimiento almacenado o función que vaya más allá de un select, insert, update o delete, ó que afecte a dos o más tablas, debe existir un diagrama de actividad.*
>
> *4º. En los casos en los que una vista, procedimiento o función utilice o se relacione con cualquier otro objeto en la base de datos distinto a tablas, deberá realizarse un diagrama de colaboración de dicha relación, haciendo mención de los parámetros enviados y recibidos, y los tipos de datos de dichos parámetros, de tal manera que el DBA pueda determinar con solo ver este diagrama que otros componentes de la base de datos se ven afectados al modificar o eliminar una objeto determinado.*

Se recomienda que los puntos 3º y 4º se adjunten a la documentación una vez concluida la fase de desarrollo del sistema.

En el momento en que cualquier cambio a los objetos de las bases de datos modificara cualquiera de los diagramas mencionados, estos deberán ser actualizados inmediatamente.

Con este se busca estandarizar aspectos relevantes de los objetos como el uso de nombres, documentación, seguridad, y rendimiento. La implementación de los estándares en este manual es de seguimiento obligatorio para todas las Bases de Datos del Ministerio. [3]"

Sin embargo de la revisión realizada, se determinó que no se ha implementado dicho estándar. Al respecto, únicamente se cuenta con un "diagrama entidad relación"[4].

4.8 OBSERVACIÓN 8: AUSENCIA DE UN PLAN FORMAL DE ADMINISTRACIÓN DE LA CAPACIDAD Y DESEMPEÑO DE LA PLATAFORMA TECNOLÓGICA

CONDICIÓN:

Actualmente no se cuenta con un plan debidamente documentado que permita la administración de la capacidad y desempeño de la plataforma tecnológica del SFE.

5. DEBILIDADES EN LA ADMINISTRACIÓN DE RIESGOS

5.1 OBSERVACIÓN 1: NO SE HA DESARROLLADO UNA METODOLOGÍA FORMAL PARA LA ADMINISTRACIÓN DEL RIESGO INFORMÁTICO.

CONDICIÓN:

Al momento de valorar la gestión del riesgo institucional se nos informó que la elaboración del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) está siendo desarrollado, el cual incluye los riesgos tecnológicos.

[3] Documento Estándares DBA, área análisis y diseño de sistemas SFE
[4] Un **diagrama o modelo entidad-relación** (a veces denominado por su siglas, *E-R* "Entity relationship", o, "DER" Diagrama de Entidad Relación) es una herramienta para el modelado de datos de un sistema de información. Estos modelos expresan entidades relevantes para un sistema de información así como sus interrelaciones y propiedades.

5.2. OBSERVACIÓN 2: NO EXISTEN PÓLIZAS PARA LOS SERVIDORES DEL SFE.

CONDICIÓN:

Al efectuar la revisión de los seguros computacionales para los equipos críticos como servidores del SFE se determinó que estas pólizas no existen.

I. INTRODUCCIÓN

1.1. ORIGEN DEL ESTUDIO.

El presente estudio denominado "Evaluación del Sistema de Control Interno Relativo a los Procesos Informáticos del Servicio Fitosanitario del Estado" de ahora en adelante (SFE), se llevó a cabo en atención al Plan Anual de Labores de la Auditoría Interna correspondiente al año 2009, específicamente en lo que corresponde al punto 2.5.5.

Mediante contratación directa 2009-20167, la Auditoría Interna del SFE a través de la Proveeduría Institucional del Ministerio de Agricultura y Ganadería promovió la "Contratación de servicios profesionales de contadores públicos autorizados y de profesionales en informática para evaluar el sistema de control interno en el SFE".

El presente informe recoge los resultados obtenidos de la evaluación de los controles internos en el área de Tecnologías de Información del SFE.

1.2. OBJECTIVO DEL ESTUDIO

Evaluar el sistema de control interno relativo a los procesos informáticos del Servicio Fitosanitario del Estado, con el propósito de determinar si el mismo está en conformidad con el ordenamiento jurídico y técnico vigente.

1.3. ALCANCE

1.3.1. Análisis de la gestión emprendida por la administración activa respecto a diseñar, mantener, perfeccionar y evaluar el sistema de control interno de la Sección de Informática del SFE, específicamente en cuanto a los procesos bajo su responsabilidad (incluye la adquisición, desarrollo y mantenimiento de sistemas de información computadorizada), en cumplimiento de lo que establece la Ley General de Control Interno N° 8292 y el "Manual de normas generales y de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización" (M-1-2002-CO-DDI), considerando las medidas que se están adoptando en la implementación de las "Normas de control interno para el sector público" (N-2-2009-CO-DFOE).

1.3.2. Análisis de la gestión emprendida por la administración activa a efecto de determinar el grado de implementación de las "Normas técnicas para la gestión y el control de las tecnologías de información" (N-2-2007-CO-DFOE).

1.3.3. Identificación de los sistemas que en el SFE están siendo adquiridos externamente (contratación administrativa) o desarrollados por la Sección de Informática del SFE, consignando el estado en que se encuentran (diseño, desarrollo, pruebas y en operación). Determinaremos si se está cumpliendo en forma razonable con los cronogramas de implementación definidos para cada uno de los sistemas.

1.3.4. Acorde con lo requerido en el inciso C.1 , C.2 y C.3 anteriores, se consideró para cada sistema identificado, el estado de conservación de la documentación física y digital que los soporta (según la técnica aplicable), tomando en cuenta aspectos relacionados con la seguridad de esa documentación, los respaldos de las respectivas bases de datos y programas fuentes. En el caso de los sistemas de información computadorizada que estén siendo desarrollados, tanto por la Sección de Informática del Servicio Fitosanitario del Estado, como por empresas externas, realizaremos pruebas para hacer una comprobación del funcionamiento de los controles que se les ha incorporado.

1.3.5. Realización de pruebas de auditoría informática a los sistemas de información computadorizada que están actualmente en operación, utilizando transacciones del semestre anterior a la fecha de inicio del estudio, para determinar si los mismos cuentan con controles adecuados y verificar que estén funcionando.

1.3.6. Se dio seguimiento a la implementación de las recomendaciones contenidas en los informes de auditoría que fueron comunicados en su oportunidad por la Auditoría Interna del MAG a la administración activa mediante el oficio AI 307-2003 de fecha 19/12/2003, con el propósito de determinar el grado de cumplimiento.

1.4. NORMAS TÉCNICAS DE AUDITORIA

En la ejecución de la presente auditoría se observaron en lo aplicable, las regulaciones establecidas para las Auditorías Internas en la Ley General de Control Interno Nº 8292, normas técnicas, directrices y resoluciones emitidas por la Contraloría General de la República.

1.5. PERIODO DEL ESTUDIO

El estudio fue efectuado durante los meses de Octubre y Noviembre del año 2009.

1.6. LIMITACIONES DEL ESTUDIO

Para este informe no se nos suministró por parte del área de Recursos Humanos del SFE la siguiente información:

- Listado del personal que ha cambiado de puesto en el Servicio Fitosanitario del Estado.
- Personal que ha sido despido o renunció al SFE.
- Colaboradores que han tenido tiempos prolongados de incapacidades o de vacaciones.
- Detalle del periodo de fechas de cada uno de los puntos anteriormente solicitados correspondientes al año 2009.

Lo anterior nos imposibilitó poder detectar si existen funcionarios del SFE con permisos o roles en la plataforma tecnológica que no fueron modificados en su momento debido a rotación de puestos, despidos, renuncias o incapacidades prolongadas, así como privilegios que no corresponden a sus funciones.

COMENTARIOS DE LA ADMINISTRACIÓN

Haciendo una revisión de los requerimientos resulta humanamente imposible brindarle la información, lo anterior por cuanto no tenemos una base de datos que registre cada uno de los movimientos solicitados. Eso habría que empezar uno por uno de los funcionarios actuales, los despedidos, etc. y según lo indicado por su persona lo requieren para los próximos días[5].

1.7. COMUNICACIÓN VERBAL DE LOS RESULTADOS

Los resultados del presente estudio fueron comentados con varios funcionarios del SFE, según se muestra en el Acta de Conferencia Final de fecha 14/12/2009. Entre esos servidores, estuvieron presentes: Ing. Gabriela Zúñiga Valerín, Directora el SFE, Ing. Carlos Padilla Bonilla, Subdirector del SFE y Ing. Didier Suárez Chaves, Jefe Sección de Informática del SFE.

[5] Este comentario fue realizado por la encargada de la Sección de Recursos Humanos del SFE.

II. OPORTUNIDADES DE MEJORA IDENTIFICADAS EN LA EVALUACIÓN CORREGIR EL ASPECTO DE LA NUMERACIÓN, TAL Y COMO SE SEÑALO EN EL CAPÍTULO ANTERIOR.

2.1. DEBILIDADES EN LA ADMINISTRACIÓN DE TI, CALIDAD Y SERVICIOS.

2.1.1. OBSERVACIÓN 1: NO SE CUENTA CON UNA METODOLOGÍA PARA LA GESTIÓN DE LA CALIDAD

2.1.1.1. CRITERIO:

La Normativa "Gestión de la Calidad" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona:" La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo."

REFERENCIA A COBIT	PO8 Administrar la calidad
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Sistema de administración de calidad. • Estándares y prácticas de calidad. • Estándares de desarrollo y de adquisición. • Enfoque en el cliente. • Mejora continua. • Medición, monitoreo y revisión de la calidad.

La Normativa "Calidad de la información" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona: "El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.

Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad."

2.1.1.2. CONDICIÓN:

Actualmente la Sección de Informática del SFE no cuenta con una metodología para la gestión de la calidad en procesos informáticos.

Se determinó que dicha Sección para comprobar la calidad y el buen funcionamiento de los sistemas y procesos en general, basa su gestión únicamente en pruebas satisfactorias y en la información de los contratos.

2.1.1.3. CAUSA:

La Sección de TI del SFE se basa en pruebas no documentadas o en la información de los respectivos contratos para comprobar la calidad de los servicios prestados, sin embargo no se cuenta con un estándar o metodología de la calidad debidamente aprobada, documentada y en ejecución, tal y como lo mencionan las normas técnicas de la Contraloría General de la República.

2.1.1.4. EFECTO:

Se corre el riesgo de que los servicios brindados y recibidos de T.I. no sean de conformidad con las necesidades presentes en las distintas secciones y departamentos del SFE, afectando los procesos tanto internos como externos.

2.1.1.5. RECOMENDACIÓN:

2.1.1.5.1. Establecer una política de aseguramiento de la calidad a nivel de la Sección de Informática del SFE, que considere entre otros aspectos lo siguiente:

- Definición de objetivos de calidad.
- Implementación de un sistema de administración de la “calidad estándar”, con enfoque en el cliente y sus necesidades.
- Establecimiento de estándares actualizados para todo el desarrollo y adquisición de software, durante todo su ciclo de vida.

2.2. DEBILIDADES VINCULADAS CON EL GOBIERNO DE T.I.

2.2.1. OBSERVACIÓN 1: NO SE CUENTA CON UNA POLÍTICA ORGANIZACIONAL PARA CONCENTRAR LA FUNCIÓN DE ADQUISICIÓN Y ADMINISTRACIÓN DE TECNOLÓGICA EN LA SECCIÓN DE INFORMÁTICA DEL SFE.

2.2.1.1. CRITERIO:

La Normativa "Implementación de Infraestructura Tecnológica" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona:" La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos."

REFERENCIA A COBIT	*AI 3 Adquirir y mantener la infraestructura tecnológica*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Plan de adquisición de infraestructura tecnológica. • Protección y disponibilidad del recurso de infraestructura. • Mantenimiento de la infraestructura. • Ambiente de prueba de factibilidad.

La Normativa "Armonización de los sistemas de información con los objetivos" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI. La adecuación de tales sistemas a los objetivos institucionales involucra, entre otros, su desarrollo de conformidad con el plan estratégico institucional, y con el marco estratégico de las tecnologías de información, cuando se haga uso de estas para su funcionamiento."

2.2.1.2. CONDICIÓN:

Según la información obtenida, parece ser que actualmente se toma en cuenta el criterio de la Sección de Informática a la hora de adquirir o mejorar la infraestructura tecnológica (Software y Hardware) del SFE. Sin embargo, no existe una política a nivel del SFE en donde se establezca la responsabilidad de que sea la citada Sección la encargada de asesorar en la implementación de la mencionada política y de velar por el cumplimiento de la misma (adquirir, administrar y mantener la plataforma tecnológica), en coordinación con las áreas usuarias.

2.2.1.3. CAUSA:

Actualmente se toma el parecer a la sección de informática a la hora de adquirir o mejorar la infraestructura tecnológica (Software y Hardware) institucional, sin embargo no existe una política a nivel del SFE en donde se establezca la responsabilidad de que sea esta sección la encargada de adquirir, administrar y mantener la plataforma tecnológica, en coordinación con las áreas usuarias, tal y como lo mencionan las normas técnicas y las normas generales de control interno, emitidas por la Contraloría General de la República.

2.2.1.4. EFECTO:

Se corre el riesgo de que las áreas usuarias implementen soluciones informáticas o adquieran recursos tecnológicos sin la aprobación de la parte técnica como lo es la sección de informática, aumentando el riesgo de incompatibilidades con las tecnologías existente y por ende el desperdicio de recursos.

2.2.1.5. RECOMENDACIÓN:

2.2.1.5.1. Elaborar, aprobar y divulgar una política a nivel institucional en donde se defina a la Sección de Informática como órgano regulador, verificador y administrador de los recursos informáticos.

2.2.2. OBSERVACIÓN 2: POCA EJECUTORÍA ACTIVA DE LA COMISIÓN INFORMÁTICA.

2.2.2.1. CRITERIO:

El apartado "Decisiones Sobre Asuntos Estratégicos de T.I." presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: "El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización."

REFERENCIA A COBIT	*PO 4 Definir procesos, organización y relaciones de TI*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Ubicación organizacional de la función de TI y estructura organizacional. • Roles y responsabilidades en calidad, riesgo, seguridad y cumplimiento. • Propiedad de datos y de sistemas. • Supervisión y relaciones externas. • Personal y personal clave de TI: segregación de funciones. • Políticas y procedimientos para personal contratado.

2.2.2.2. CONDICIÓN:

De acuerdo con la revisión realizada a la estructura organizacional para la administración de los recursos informáticos, se observó que el SFE cuenta con una Comisión para la gestión informática. Sin embargo, esta Comisión sólo se ha reunido una vez en el presente año, con el fin de comparar los equipos solicitados por los diferentes departamentos con los inventarios actualizados del equipo de cómputo que posee la Sección de Informática. Cabe mencionar además que no se cuenta con ningún documento de conformación de la Comisión ni con un reglamento en donde se especifique las funciones de la misma, la periodicidad de las reuniones y miembros que la conforman, entre otros aspectos relevantes.

2.2.2.3. CAUSA:

Si bien es cierto existieron en su momento directrices verbales por parte del Director del SFE para la conformación de la Comisión Informática poco a poco los representantes de los departamentos dejaron de asistir a las reuniones, incumpliendo instrucciones superiores por parte de los miembros de la Comisión.

2.2.2.4. EFECTO:

El SFE no está logrando un equilibrio en la asignación de recursos y en la adecuada atención de los requerimientos de todas las unidades de la organización.

2.2.2.5. RECOMENDACIONES:

2.2.2.5.1. Reanudar las reuniones y asesoría activa de la Comisión Informática, con el fin de asegurar las actividades de control interno en materia tecnológica, para que el jerarca pueda apoyar sus decisiones sobre asuntos estratégicos de T.I en concordancia con la estrategia institucional, estableciendo prioridades, y un equilibrio en la asignación de recursos.

2.2.2.5.2. Establecer el reglamento (o documento similar), en el cual se establezca entre otros aspectos la razón de ser de la citada Comisión, conformación y estructura de operación, funciones, integrantes y responsabilidades.

2.2.2.5.3. Remitir para razón de apertura a la Auditoría Interna del SFE, el libro de actas que deberá mantener en forma actualizada la Comisión de Informática del SFE.

2.2.3. OBSERVACIÓN 3: NO SE CUENTA CON UN PLAN ESTRATÉGICO A LARGO PLAZO PARA LA SECCIÓN DE INFORMÁTICA DEL SFE.

2.2.3.1. CRITERIO:

La Normativa "Planificación de la Tecnologías de Información" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, dice: "La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes."

REFERENCIA A COBIT	*PO 1 Definir el plan estratégico de TI*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Administración del valor de TI. • Alineación de TI con el negocio. • Evaluación del desempeño actual. • Planes tácticos de TI. • Administración del portafolio de TI.

La Normativa "Armonización de los sistemas de información con los objetivos" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI. La adecuación de tales sistemas a los objetivos institucionales involucra, entre otros, su desarrollo de conformidad con el plan estratégico institucional, y con el marco estratégico de las tecnologías de información, cuando se haga uso de estas para su funcionamiento."

2.2.3.2. CONDICIÓN:

Al efectuar la revisión de la administración y planificación de los recursos informáticos del SFE, se determinó que aún no se ha elaborado un plan estratégico a largo plazo de tecnologías de información. Actualmente el SFE solamente cuenta con un Plan Operativo Institucional (POI).

Cabe mencionar que el SFE está por aprobar un plan estratégico a largo plazo, esto como producto del proceso de modernización que se está llevando a cabo, por lo que el plan a largo plazo de informática debe estar ligado con el plan estratégico institucional.

2.2.3.3. CAUSA:

En el pasado el SFE no dedicó el tiempo suficiente para elaborar un plan estratégico institucional a largo plazo, situación que no le ha permitido al SFE implementar un PETI (Plan Estratégico de T.I.), ya que este último toma como insumo el primero, incumpliendo con las normas técnicas emitidas por la Contraloría General de la República.

2.2.3.4. EFECTO:

No se tiene claro el rumbo que debe seguir la Sección de Informática respecto a las tecnologías de información para los años venideros, lo que pone en riesgo el cumplimiento efectivo de las metas y objetivos institucionales.

2.2.3.5. RECOMENDACIÓN:

2.2.3.5.1. Elaborar un plan estratégico de tecnologías de información, el cual deberá estar debidamente alineado con el plan estratégico institucional que está próximo a aprobarse; lo anterior con el fin de mejorar la administración de los recursos informáticos, estableciendo el presente tecnológico institucional y hacia donde se pretende llegar en materia tecnológica, para ello se debe implementar un conjunto de acciones que sean medibles a lo largo de la implementación del citado plan estratégico en T.I.

2.2.4. OBSERVACIÓN 4: SE CARECE DE UN MANUAL DE FUNCIONES PARA LA SECCIÓN DE INFORMÁTICA DEL SFE.

2.2.4.1. CRITERIO:

El objetivo de control (CobiT®) PO4.11 – Segregación de Funciones explica que: "Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un sólo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas."

La Normativa "Separación de funciones incompatibles y del procesamiento de transacciones" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona: "El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la Institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores. Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables."

2.2.4.2. CONDICIÓN:

Al efectuar la revisión sobre las cargas de trabajo de los colaboradores de la Sección de Informática, se determinó que no existe un manual de funciones para cada unos de los cargos establecidos en dicha Sección. Actualmente el SFE, únicamente cuenta con el "Manual de Clases Anchas" de la Dirección General de Servicio Civil.

2.2.4.3. CAUSA:

El SFE a la fecha no ha visualizado la necesidad de contar con funciones específicas para cada uno de los cargos que conforman la Sección de Informática del SFE.

2.2.4.4. EFECTO:

No están documentadas las funciones realizadas por el personal de la sección de informática, lo que podría ocasionar:

1. No se facilita la comprensión de los objetivos, políticas, estructuras y funciones de cada integrante de la sección.
2. No están plenamente definidas las funciones y responsabilidades de cada miembro de la sección.
3. No se asegura y facilita al personal la información necesaria para realizar las labores que les han sido encomendadas y lograr la uniformidad en los procedimientos de trabajo y la eficiencia y calidad esperada en los servicios.
4. Se dificulta el ahorro de tiempos y esfuerzos de los funcionarios, evitando funciones de control y supervisión innecesarias.
5. Podría existir desperdicios de recursos humanos y materiales.
6. No se facilita la selección de nuevos empleados ni se les proporciona los lineamientos necesarios para el desempeño de sus atribuciones.
7. No se constituye en una base para el análisis posterior del trabajo y el mejoramiento de los sistemas y procedimientos.
8. No se delimitan claramente las responsabilidades de cada área de trabajo, lo que podría evitar conflictos inter-estructurales.

2.2.4.5. RECOMENDACIÓN:

2.2.4.5.1. Elaborar un manual de funciones para los colaboradores de la Sección de Informática del SFE, con el fin de poder determinar entre otros aspectos claramente las cargas de trabajo, la comprensión de las responsabilidades y funciones establecidas, facilitar la capacitación de los nuevos integrantes, lograr la uniformidad de los procesos de trabajo, ahorrar tiempos y esfuerzos, evitar pérdidas de recursos, logrando un análisis cuantitativo de las labores y el mejoramiento de las tareas realizadas.

2.2.5. OBSERVACIÓN 5: INADECUADA SEGREGACIÓN DE FUNCIONES PARA EL ENCARGADO DE ADMINISTRAR LAS BASES DE DATOS DEL SFE.

2.2.5.1. CRITERIO:

La Normativa "Independencia y Recurso Humano de la Función de TI" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)"de la Contraloría General de la República, dice: " Se debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones."

REFERENCIA A COBIT	*PO 4, Definir procesos, organización y relaciones de TI,* *PO 7 Administrar recursos humanos de TI*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Ubicación organizacional de la función de TI y estructura organizacional. • Roles y responsabilidades en calidad, riesgo, seguridad y cumplimiento. • Propiedad de datos y de sistemas. • Supervisión y relaciones externas. • Personal y personal clave de TI: segregación de funciones. • Políticas y procedimientos para personal contratado. • Reclutamiento y retención del personal. • Competencias del personal. • Asignación de roles. • Entrenamiento del personal de TI. • Dependencia sobre los individuos. • Procedimientos de Investigación del personal. • Evaluación del desempeño del empleado. • Cambios y terminación de trabajo.

La Normativa "Separación de funciones incompatibles y del procesamiento de transacciones" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona: "El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la Institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores. Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables."

2.2.5.2. CONDICIÓN:

Al efectuar el estudio sobre las funciones realizadas por el personal de la Sección de Informática, se determinó que dicha Sección no cuenta en su estructura organizacional interna con un puesto de administrador de bases de datos (DBA). Dicha función la está ejerciendo un funcionario del área de "Análisis y Desarrollo de Sistemas", quién a su vez realiza funciones de desarrollador de sistemas.

2.2.5.3. CAUSA:

La Sección de Informática del SFE no ha visualizado la necesidad de contar con un puesto de DBA como parte de su estructura organizativa.

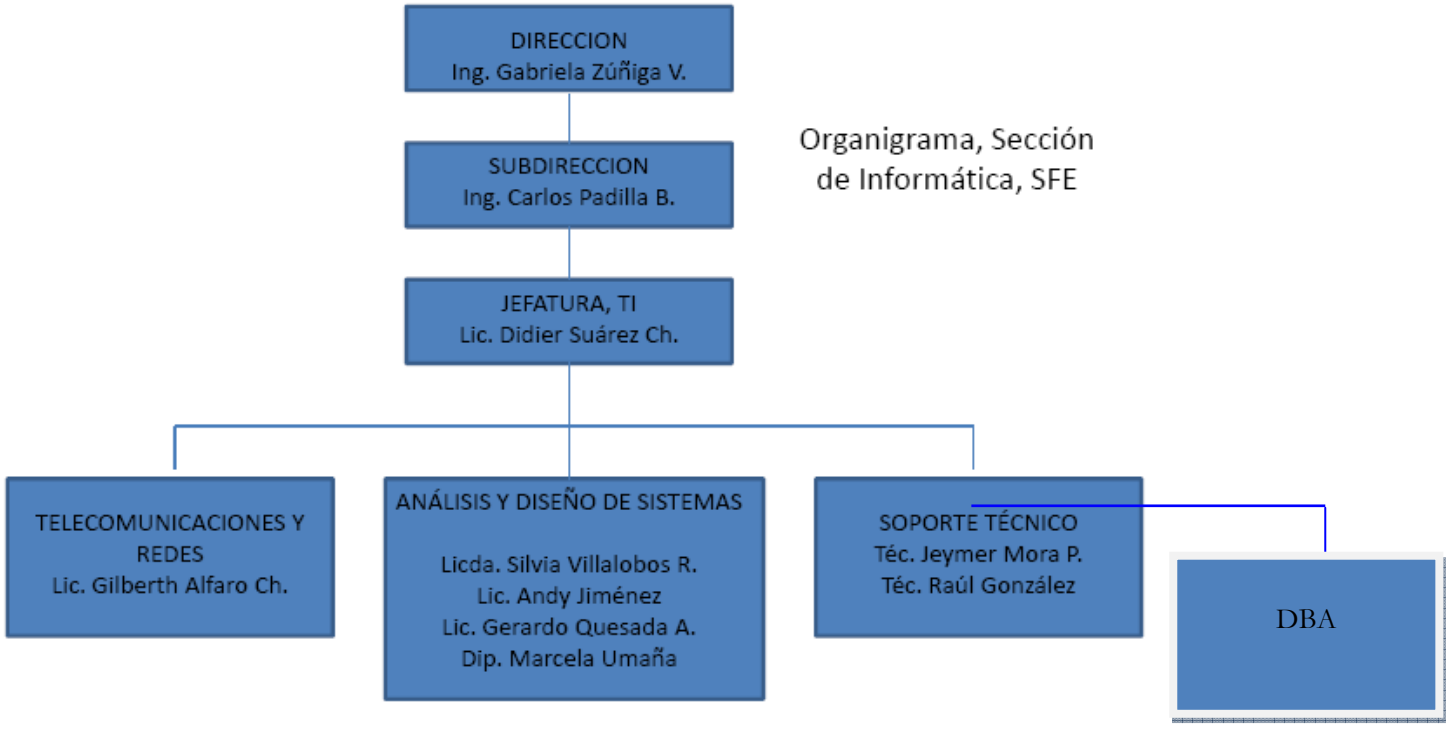
2.2.5.4. EFECTO:

Al no contar con un DBA a tiempo completo y exclusivo para las labores de bases de datos, los tiempos de espera para la realización de las distintas tareas de bases de datos aumentan, además se corre el riesgo de manipulación de la información, se da una inadecuada segregación de funciones y no se genera una adecuada seguridad de los datos.

2.2.5.5. RECOMENDACIONES:

2.2.5.5.1. Dotar a la Sección de Informática del SFE de una plaza con el perfil para DBA, con el fin de establecer una adecuada segregación de funciones en la manipulación de las bases de datos institucionales. Mientras se realizan las gestiones que posibiliten la asignación de dicho puesto, se deben tomar las medidas pertinentes, que permitan asignar las funciones de DBA a un funcionario con el perfil adecuado, y que no se violente la normativa relativa a la segregación de funciones y que no se ponga en peligro la seguridad de los datos. La decisión que adopte la administración debe quedar debidamente fundamentada y documentada.

2.2.5.5.2. Crear un área funcional denominada "Administración de Bases de Datos" (DBA) como parte de la estructura organizativa de la Sección de Informática del SFE, quedando el organigrama interno de T.I. de la manera que se muestra seguidamente. La decisión que adopte la administración debe quedar debidamente fundamentada y documentada.



Organigrama, Sección de Informática, SFE

2.2.6. OBSERVACIÓN 6: NO SE CUENTA CON UNA BASE DE DATOS DE CONOCIMIENTO PARA EL AREA DE TI.

2.2.6.1. CRITERIO:

Las Bases de Datos de Conocimiento representan una guía práctica que se utiliza como herramienta de soporte para la organización y comunicación, que contiene información ordenada y sistemática, en la cual se establecen claramente los objetivos, procedimientos, funciones e implementación de un problema ya presentado en la organización, lo que hace que sean de mucha utilidad para lograr una eficiente administración. Este tipo de herramientas facilitan el aprendizaje y proporcionan la orientación precisa que requiere la acción humana en cada una de las unidades administrativas que conforman a las organizaciones, fundamentalmente a nivel operativo o de ejecución, pues son una fuente de información que trata de orientar y mejorar los esfuerzos de sus integrantes para lograr la adecuada realización de las actividades.

2.2.6.2. CONDICIÓN:

El SFE no ha implementado una base de datos que le posibilite registrar el conocimiento y la resolución de problemas específicos relacionados con las tecnologías de información. Esta base debe informar y orientar sobre la forma de utilizar dichas tecnologías a nivel organizacional, unificando los criterios de desempeño y cursos de acción que deben seguirse para cumplir con los objetivos planteados; además de poder agrupar el conocimiento de las diferentes áreas usuarias del SFE.

2.2.6.3. CAUSA:

No se ha valorado la posibilidad a nivel del SFE de poder implementar una Base de Datos de conocimiento de problemas comunes, agrupando además la resolución de problemas presentados en áreas específicas del servicio.

2.2.6.4. EFECTOS:

1. No se asegura y facilita al personal la información necesaria para poder realizar una tarea específica en el área de T.I de una manera eficiente y autodidacta.

2. Se dificulta el ahorro de tiempos y esfuerzos de los funcionarios del área de T.I al estar atendiendo problemas comunes.

3. No se cuenta con una base para el análisis posterior del trabajo y el mejoramiento de los sistemas y procedimientos.

2.2.6.5. RECOMENDACIÓN:

2.2.6.5.1. Crear una Base de Datos del conocimiento para el SFE en donde se pueda buscar la respuesta a una problemática ya resuelta para que sea empleada por todos los miembros de la organización, optimizando el tiempo de los funcionarios de T.I. y agrupando el conocimiento que a través de los años se ha generado en las distintas áreas usuarias.

2.3. DEBILIDADES EN LA SEGURIDAD DE T.I.

2.3.1 OBSERVACIÓN 1: NO SE TIENE LA PRÁCTICA DE COMUNICAR EN FORMA PERIODICA Y CONSTANTE CAMBIOS DE PERSONAL EN EL SFE A LA SECCIÓN DE INFORMÁTICA.

2.3.1.1. CRITERIO:

La Normativa “Gestión de la seguridad de la información” presente en el documento “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)” de la Contraloría General de la República, menciona:” La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- La implementación de un marco de seguridad de la información.
- El compromiso del personal con la seguridad de la información.
- La seguridad física y ambiental.
- La seguridad en las operaciones y comunicaciones.
- El control de acceso.
- La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
- La continuidad de los servicios de TI.

Además debe establecer las medidas de seguridad relacionadas con:

- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
- El manejo de la documentación.
- La terminación normal de contratos, su rescisión o resolución.
- La salud y seguridad del personal.

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados."

REFERENCIA A COBIT	*DS 5 Garantizar la seguridad de los sistemas*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Administración de la seguridad de TI. • Plan de seguridad de TI. • Administración de identidad. • Administración de cuentas del usuario. • Pruebas, vigilancia y monitoreo de la seguridad. • Definición de incidente de seguridad. • Protección de la tecnología de seguridad. • Administración de llaves criptográficas. • Prevención, detección y corrección de software malicioso. • Seguridad de la red. • Intercambio de datos sensitivos.

2.3.1.2. CONDICIÓN:

Actualmente no se cuenta a nivel organizacional con una política en donde se defina que la Sección de Recursos Humanos del SFE debe suministrar periódicamente a la Sección de Informática un listado de las personas que han tenido alguna rotación en los distintos puestos del SFE (renuncias, despidos o vacaciones prolongadas, etc), con el fin de realizar los respectivos cambios de roles y privilegios en los sistemas de información y la red.

2.3.1.3. CAUSA:

Falta de una política orientada al suministro de información oportuna por parte de la Sección de Recursos Humanos a la Sección de Informática, ambas dependencias del SFE.

2.3.1.4. EFECTO:

Se corre el riesgo de que exista fuga y manipulación indebida de información, al no estar bien definidos los roles y privilegios de los sistemas de información y de la red del SFE.

2.3.1.5. RECOMENDACIÓN:

2.3.1.5.1. Elaborar, aprobar y divulgar una política, mediante la cual la Sección de Recursos Humanos del SFE remita en forma periódica información a la Sección de Informática relacionada con movimientos de personal (que han cambiado de puestos, gozan de periodos de vacaciones o incapacidades prolongadas -mayores a 15 días-, renuncias o despidos, etc), con el fin de que el área de informática tome las medidas pertinentes con respecto a la definición de roles y privilegios de los sistemas de información y de la red del SFE.

2.3.2. OBSERVACIÓN 2: EL ÁREA EN DONDE SE ENCUENTRAN LOS SERVIDORES DEL SFE NO CUENTA CON UNA ADECUADA SEGURIDAD.

2.3.2.1. CRITERIO:

La Normativa “DS12 Administrar el Ambiente Físico” presente en el documento COBIT menciona: “La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.”. La Normativa “Seguridad” presente en el documento “Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)” de la Contraloría General de la República, menciona:” Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.”

2.3.2.2. CONDICIÓN:

Al efectuar la revisión del área en donde se encuentran los servidores del SFE, se determinó que no existen detectores de humo, ni alarmas contra incendio, tampoco se cuenta con cámaras de vigilancia ni un deshumidificador. Es conveniente la instalación de este último dispositivo en el cuarto de servidores, ya que la humedad puede ocasionar la corrosión de los componentes internos y la degradación de propiedades tales como la resistencia eléctrica, la conductividad térmica, la resistencia física y el tamaño[6]. Además, no es conveniente que los servidores del Servicio Nacional de Salud Animal (SENASA) y la "Central Telefónica" se encuentre en el área de servidores del SFE, por cuanto entran personas ajenas a la Sección de Informática del SFE, poniendo en riesgo la información almacenada en esos servidores. Por otra parte es recomendable la instalación de un control de acceso biométrico[7] al cuarto de servidores.

2.3.2.3. CAUSA:

El cuarto en donde se ubican los servidores no cuenta con las medidas suficientes para salvaguardar al equipo de cómputo, y la información que se encuentra almacenada en los servidores, debido a la falta de espacio en la infraestructura actual y por la falta de planificación presupuestaria que no ha permitido visualizar la adquisición de dispositivos y equipos que podrían mejorar las condiciones actuales.

2.3.2.4. EFECTO:

Se corre el riesgo que personas no autorizadas entren al área de servidores pudiendo provocar daños a la información o fuga de la misma, además ante una posible contingencia como lo es un incendio no se cuenta con los mecanismos que alerten al personal para tomar las medidas del caso.

2.3.2.5. RECOMENDACIÓN:

2.3.2.5.1. Dotar a la Sección de Informática del SFE de los recursos suficientes (presupuestarios y económicos debidamente aprobados), cuya ejecución posibilite la adquisición e instalación de dispositivos y equipos en el área donde se ubican los servidores del SFE, con el propósito de mejorar la seguridad.

---

[6] Se refiera a la masa molecular del computador.

[7] La biometría es una tecnología de seguridad basada en el reconocimiento de una característica de seguridad y en el reconocimiento de una característica física e intransferible de las personas, como por ejemplo la huella digital.
Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica

2.3.3. OBSERVACIÓN 3: FALTA DOCUMENTAR EL PROCEDIMIENTO PARA DEFINIR PERFILES, ROLES Y NIVELES DE PRIVILEGIO A LOS USUARIOS DE LOS SISTEMAS IMPLANTADOS EN EL SFE.

2.3.3.1. CRITERIO:

La Normativa "Control de Acceso" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de ***necesidad de saber* o *menor privilegio*.** Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones."

REFERENCIA A COBIT	*DS 5 Garantizar la seguridad de los sistemas*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Administración de la seguridad de TI. • Plan de seguridad de TI. • Administración de identidad. • Administración de cuentas del usuario. • Pruebas, vigilancia y monitoreo de la seguridad. • Definición de incidente de seguridad. • Protección de la tecnología de seguridad. • Administración de llaves criptográficas. • Prevención, detección y corrección de software malicioso. • Seguridad de la red. • Intercambio de datos sensitivos.

La Normativa "Control de sistemas de información" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter."

2.3.3.2. CONDICIÓN:

Al efectuar la revisión de los perfiles, roles y niveles de privilegio de los usuarios de los sistemas implantados en el SFE, se determinó que actualmente ni la Sección de Informática ni las demás Unidades usuarias del SFE, cuentan con un procedimiento debidamente documentado para definir este tipo de perfiles.

2.3.3.3. CAUSA:

Falta de procedimientos para definir perfiles, roles y niveles de privilegios a los usuarios de los sistemas de información.

2.3.3.4. EFECTO:

Se corre el riesgo de que usuarios tengan asignados roles y privilegios que no le competen teniendo la posibilidad de modificar, o ver información confidencial o que no corresponde al área de trabajo en que se desempeña.

2.3.3.5. RECOMENDACIÓN:

2.3.3.5.1. Elaborar, aprobar y divulgar el procedimiento, cuya implementación le permita a los encargados de los sistemas de información la asignación de roles y privilegios a los respectivos usuarios; lo anterior con el propósito de que personal de la Sección de Informática del SFE no intervenga en dicha actividad.

2.3.4. OBSERVACIÓN 4: AUSENCIA DE SEGURIDAD EN EL SISTEMA DE PLANILLAS DEL SFE.

2.3.4.1. CRITERIO:

La Normativa "Seguridad en la implementación y mantenimiento de Software e infraestructura tecnológica" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona:"La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información. Para ello debe:

- Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
- Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
- Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
- Controlar el acceso a los programas fuente y a los datos de prueba."

REFERENCIA A COBIT	*AI 2, Adquirir y mantener el software aplicativo* *AI 3 Adquirir y mantener la infraestructura tecnológica*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Diseño de alto nivel. • Diseño detallado. • Control y auditabilidad de las aplicaciones. • Seguridad y disponibilidad de las aplicaciones. • Configuración e implantación de software aplicativo. • Actualizaciones importantes en sistemas existentes. • Desarrollo de software aplicativo. • Aseguramiento de la Calidad del Software. • Administración de los requerimientos de aplicaciones. • Mantenimiento de software aplicativo. • Plan de adquisición de infraestructura tecnológica. • Protección y disponibilidad del recurso de infraestructura. • Mantenimiento de la infraestructura. • Ambiente de prueba de factibilidad.

La Normativa "Control de sistemas de información" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter."

2.3.4.2. CONDICIÓN:

Al realizar la valoración a los sistemas de información implantados en el SFE, se determinó que el sistema de planillas esta desarrollado en FOX (lenguaje de programación que nació varias décadas atrás). Además, dicho sistema no presenta una seguridad adecuada debido a las siguientes razones:

- El sistema es portable, es decir se guarda en cualquier medio de almacenamiento externo, permitiendo instalar la aplicación en cualquier terminal.
- El sistema no solicita el cambio de clave automáticamente ni se desactiva en caso de no ser utilizado después de cierto periodo de tiempo.
- El sistema lo manipulan dos personas, las cuales cuentan con el mismo usuario y misma contraseña.
- El sistema genera archivos dbf (Base de datos), que se guardan en la máquina del usuario.
- No presenta bitácoras para verificar alguna inadecuada manipulación de la información.
- No se lleva un registro histórico de las claves.
- No existe un procedimiento automatizado o administrativo para la detección de accesos no autorizados.
- No se llevan los tiempos ni días de acceso por terminal.

Por otra parte el sistema presenta algunas limitaciones como:

- No desactiva a los empleados interinos, es decir, el encargado de la planilla debe estar revisando constantemente cuando una persona interina ya no labora para el SFE, de lo contrario la planilla de pagos se genera con esas personas.
- No calcula liquidaciones.
- No cuenta con filtros para reportes históricos.
- No presenta la posibilidad de calcular anualidades.
- No se posee el código del sistema, lo que se conoce en informática como una caja negra.
- Se depende 100% del mantenimiento por parte del proveedor.

Cabe mencionar que el Sistema de Planillas es utilizado además por el SENASA, aún cuando el propietario del sistema es el SFE; y el mantenimiento al mismo es cubierto con recursos del SFE y del SENASA. Dicha situación eventualmente podría estar generando un incumplimiento a la Ley de Protección Fitosanitaria N° 7664, por cuanto el SFE tiene la imposibilidad de compartir recursos con órganos que no estén vinculados con el cumplimiento de sus objetivos.

2.3.4.3. CAUSA:

El sistema fue desarrollado en una plataforma tecnológica que para nuestros días se puede considerar obsoleta en cuanto a las características de seguridad que presenta, además que la gestión del SFE no ha sido suficiente respecto a contar con el sistema de información requerido para la administración de las planillas de pago de su personal.

2.3.4.4. EFECTO:

Se corre el riesgo de que la información de la planilla del SFE sea manipulada por personas ajenas al área de planillas, además de que la información no sea recuperada ante una contingencia. Por otra parte existe la posibilidad de que se le pague a una persona interina a pesar de que ya no labore para el SFE.

2.3.4.5. RECOMENDACIÓN:

2.3.4.5.1. Gestionar ante el Ministerio de Hacienda la posibilidad de administrar la relación de puestos del SFE a través del Sistema denominado "INTEGRA". No obstante, en caso de no ser posible concretar dicha gestión en el corto plazo, valorar la posibilidad de adquirir (contratación de servicios profesionales) o desarrollar internamente el sistema de planillas de pago que requiere el SFE.

Mientras se toman las acciones indicadas en el párrafo anterior, el SFE con el apoyo de su Sección de Informática y la colaboración del Área de Informática del MAG, debe adoptar las medidas que se consideren necesarias, con el propósito de minimizar los efectos negativos en que está operando el sistema de información bajo la administración del Departamento de Recursos Humanos del MAG.

2.3.5. OBSERVACIÓN 5: IDENTIFICACIÓN DE USUARIOS GENÉRICOS EN LA PLATAFORMA TECNOLÓGICA

2.3.5.1. CRITERIO:

La Normativa "Control de Acceso" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de ***necesidad de saber* o *menor privilegio*.** Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones."

REFERENCIA A COBIT	*DS 5 Garantizar la seguridad de los sistemas*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Administración de la seguridad de TI. • Plan de seguridad de TI. • Administración de identidad. • Administración de cuentas del usuario. • Pruebas, vigilancia y monitoreo de la seguridad. • Definición de incidente de seguridad. • Protección de la tecnología de seguridad. • Administración de llaves criptográficas. • Prevención, detección y corrección de software malicioso. • Seguridad de la red. • Intercambio de datos sensitivos.

La Normativa "Seguridad" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" Deben instaurarse los controles que aseguren que la información que se comunica, resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."

2.3.5.2. CONDICIÓN:

Al realizar un estudio sobre los usuarios que se encuentran definidos en la plataforma tecnológica se identificó la existencia de usuarios genéricos como por ejemplo:

- Administrador Sitio Web.
- Aeropuerto.
- Cuarentena aeropuerto Daniel Oduber.
- Cuarentena Aeropuerto Tobias Bolaños.
- Cuarente Los Chiles.
- Dirección.
- Estación Cuarentena (Aeropuerto, Caldera, Golfito, Limón, Paso Canoas, Sixaola, Ventanilla Única).
- Fitosanitario (Caldera, de exportación, Limón).
- GSI.
- GTEUser.
- Laboratorio Laboratorio control calidad.
- Plaguicidas SFE.
- Prensa SFE.
- Recursos Humanos.
- Región (Brunca, Cartago, Chorotega, Esparza, Grecia, Guápiles, Huetar Norte, Puriscal).
- SICOIN.
- SICOININSTALLERUSER.
- SQL Admin.

Lo anterior provoca que en una misma terminal varios funcionarios puedan acceder a los sistemas de información con un mismo usuario, lo cual podría dificultar la determinación del responsable ante un posible mal manejo de la información.

2.3.5.3. CAUSA:

En su mayoría estas cuentas genéricas se crearon para estaciones y programas donde no todo los funcionarios contaban con equipo.

2.3.5.4. EFECTO:

Se corre el riesgo que ante una posible inadecuada manipulación de los sistemas de información no se pueda determinar al responsable.

2.3.5.5. RECOMENDACIONES:

2.3.5.5.1. Eliminar la práctica de implementar el uso de usuarios genéricos, en aquellas dependencias del SFE donde las circunstancias posibilitan la definición de usuarios específicos para cada funcionario.

2.3.5.5.2. Documentar la necesidad de crear usuarios genéricos, situación que permitirá conocer con precisión, entre otra información, el nombre del funcionario que autorizó dicho usuario, la dependencia y los funcionarios que tienen acceso a los respectivos equipos, así como la justificación respectiva.

2.3.6. OBSERVACIÓN 6: NO EXISTE UN PLAN DE CONTINGENCIAS INTEGRAL QUE AYUDE A SALVAGUARDAR LOS RECURSOS INFORMÁTICOS DEL SFE, ASÍ COMO GARANTIZAR LA CONTINUIDAD DE LAS OPERACIONES.

2.3.6.1. CRITERIO:

La Normativa "Continuidad de los servicios de TI" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)"de la Contraloría General de la República, dice: "La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad."

REFERENCIA A COBIT	*DS 4 Garantizar la continuidad del servicio*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Marco de trabajo de continuidad. • Planes de continuidad de TI. • Recursos críticos de TI. • Mantenimiento del plan de continuidad de TI. • Pruebas del plan de continuidad de TI. • Entrenamiento del plan de continuidad de TI. • Distribución del plan de continuidad de TI. • Recuperación y reanudación de los servicios de TI. • Almacenamiento de respaldos fuera de las instalaciones. • Revisión post-reanudación.

La Normativa "Valoración del riesgo" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:"El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure."

2.3.6.2. CONDICIÓN:

Según el análisis realizado a la continuidad de las operaciones, se determinó que la Sección de Informática del SFE, no cuenta con un plan de contingencias integral que en caso de imprevistos, permita la administración y utilización de los recursos tecnológicos de manera apropiada.

2.3.6.3. CAUSA:

Por la falta de tiempo y capacitación no se ha elaborado el plan de contingencias integral que requiere el SFE.

2.3.6.4. EFECTO:

No se tiene clasificados y documentados los riesgos institucionales en materia de tecnologías de información, y en caso de un contingente las acciones preventivas y correctivas necesarias para mitigar el impacto del mismo pueden ser tardíos o poco eficientes debido a la falta de planificación.

2.3.6.5. RECOMENDACIÓN:

2.3.6.5.1. Confeccionar un plan de contingencias integral en materia tecnológica para el SFE, cuya implementación permita asegurar la continuidad de los servicios que brinda la organización. Dicho plan debe ser aprobado por la máxima autoridad del SFE y ser de conocimiento por parte del personal. Lo anterior, permitirá asegurar la disponibilidad de una metodología estandarizada a nivel institucional que apoye el análisis y gestión de los riesgos para TI. A su vez, debe asegurar su adecuada aplicación, revisión y mantenimiento periódico, de forma que se garantice que la Institución pueda enfrentarse adecuadamente ante cualquier eventualidad. Además, se debe considerar entre otros aspectos, lo siguiente:

a) La constitución de un equipo de trabajo con representación de las unidades que correspondan.

b) La designación de un responsable del proceso de implementación, quién asumirá la coordinación del equipo de trabajo y deberá contar con la autoridad necesaria, dentro de sus competencias, para ejecutar el referido plan.

c) El estudio detallado de las normas técnicas emitidas por la Contraloría General de la República, con el fin de identificar las que apliquen a la Institución de conformidad con su realidad tecnológica y con base en ello establecer las prioridades respecto de su implementación.

d) Dicha planificación deberá considerar las actividades por realizar, los plazos establecidos para cada una de las tareas, los respectivos responsables, los costos estimados, así como cualquier otro requerimiento asociado (tales como infraestructura, personal y recursos técnicos) y quedar debidamente documentada.

Este plan debe definir una serie de procedimientos organizados por área (servidores, programación, quiebra proveedor, caídas del sistema, reposición de equipos, administración de la red, etc.). Asimismo, se deben establecer los objetivos para cada procedimiento, con un detalle de los pasos a seguir y responsables.

Además el plan debe contener medidas preventivas como por ejemplo contratos con otros proveedores, mantenimiento preventivo, bitácoras para el acceso a los servidores, etc. También se deben definir los riesgos, clasificarlos, identificarlos (aceptación, eliminación, reducción, transferencia del riesgo), se debe analizar el impacto de los riesgos, tomando en cuenta el tiempo de recuperación, la probabilidad que ocurra un riesgo, así como la implementación de planes de entrenamiento y pruebas para el personal.

COMENTARIOS DE LA ADMINISTRACIÓN:

No se ha elaborado por falta de tiempo y capacitación de un plan de contingencia y continuidad formalmente esquematizado. Tampoco se ha elaborado una matriz completa de todos los riesgos en materia de TI: sin embargo, se han evaluado los riesgos más críticos y en la medida de lo posible hemos buscado opciones para mitigarlos. Al respecto, recientemente se han adquirido equipos y servicios, tales como; nuevos servidores, mejora en los enlaces remotos con las estaciones de todo el país, enlaces alternos en las principales estaciones para conexión con oficinas del Ministerio de Hacienda para poder transmitir al TICA en caso de interrupción con el enlace central, compra de UPS con mayor capacidad, se cambiaron los switches y enrutadores en las estaciones remotas, se adjudicó un contrato de asistencia en soporte a nuestra plataforma Microsoft, se renovó el contrato de una caja de seguridad en un Banco privado a fin de mantener un respaldo fuera del sitio, y actualmente se están evaluando alternativas de vitalización de servidores de datos, para mitigar el riesgo de fallo en los servicios que brindamos.

2.3.7. OBSERVACIÓN 7: NO EXISTE UN MECANISMO DE REPLICACIÓN AUTOMÁTICA EXTERNO PARA LOS SERVIDORES PRINCIPALES DEL SFE.

2.3.7.1. CRITERIO:

La Normativa "DS4.1 IT Marco de trabajo de continuidad" presente en el documento COBIT menciona:" Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI.".

La Normativa "Oportunidad" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" Las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales."

2.3.7.2. CONDICIÓN:

Al efectuar la revisión de los respaldos de la información almacenada en los servidores del SFE, se determinó que no se cuenta con un mecanismo de replicación automática en un lugar externo a las instalaciones del SFE. Dicha situación no estaría permitiendo garantizar la continuidad de las operaciones en forma inmediata en caso de falla del servidor principal localizado en oficinas centrales del SFE ubicadas en el Barreal de Heredia.

2.3.7.3. CAUSA:

La gestión emprendida por el SFE para la continuidad de las operaciones no ha sido suficiente, situación que no ha permitido contar un mecanismo que posibilite la continuidad de los servicios que brinda el SFE.

2.3.7.4. EFECTO:

Al presentarse alguna falla en el servidor principal no se cuenta con el equipo adecuado para la continuidad inmediata de las operaciones en el SFE, pudiendo generar la paralización de las operaciones por varias horas ocasionando además la posible pérdida de información valiosa.

2.3.7.5. RECOMENDACIÓN:

2.3.7.5.1. Valorar la posibilidad de dotar a la Sección de Informática del SFE, del equipo necesario para poder implementar un mecanismo de replicación automática en un sitio alterno (bajo un enfoque de costo-beneficio), para que en caso de fallas del servidor principal, el equipo de respaldo entre a funcionar de forma inmediata impidiendo la paralización de las operaciones. Para la efectividad de lo recomendado, se debe contar además con un ancho de banda adecuado y una infraestructura de comunicaciones apropiada para evitar caídas de la red.

Además, una vez se cuente con el equipo necesario, se debe agregar al plan de contingencia integral (cuando se elabore y apruebe) los procedimientos para realizar el respaldo en espejo, implementar un plan de pruebas y ejecutarlo cada cierto periodo de tiempo para garantizar que el equipo va a funcionar adecuadamente en caso de un contingente.

2.3.8. OBSERVACIÓN 8: POCO ESPACIO FÍSICO PARA LA SECCIÓN DE INFORMÁTICA.

2.3.8.1. CRITERIO:

La Normativa "DS12 Administración del Espacio Físico" presente en el documento COBIT menciona:" La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.".

2.3.8.2. CONDICIÓN:

El espacio físico con que cuenta la Sección de Informática del SFE es insuficiente para albergar adecuadamente la cantidad de recurso humano y equipo técnico. No obstante, el SFE tiene prevista la asignación de mayor espacio físico para la citada Sección, en el edificio que se está remodelando; situación que según la jefatura de esa área estaría mejorando las condiciones existentes.

2.3.8.3. CAUSA:

El área en donde se encuentra la sección de informática no es el suficiente, aunado a un inadecuado diseño del espacio físico.

2.3.8.4. EFECTO:

Las condiciones actuales podrían provocar efectos negativos en la salud de los funcionarios y una eventual disminución de su capacidad productiva.

2.3.8.5. RECOMENDACIÓN:

2.3.8.5.1. Dotar a la Sección de Informática del SFE de un área que cuente con un diseño y espacio necesario para poder administrar los recursos de TI de la mejor manera, permitiendo al personal realizar gestiones administrativas y de servicio de los funcionarios del SFE. También se debe asignar una zona específica con acceso restringido para ubicar los equipos, herramientas y otros dispositivos requeridos para la instalación, revisión y/o reparación de hardware, así como mobiliario apropiado que asegure la prevención de accidentes y posibles daños a los activos que en esta área se ubiquen, así como la adecuada comodidad para que los funcionarios desarrollen sus labores en forma segura y saludable, tomando en cuenta factores ambientales y estructurales con el fin de disminuir los posibles riesgos ocasionados por fuego, rayos, inundaciones, etc.

2.3.9. OBSERVACIÓN 9: NO SE CUENTA CON UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN).

2.3.9.1. CRITERIO:

La Normativa "ME1 Monitorear y evaluar el desempeño de TI" presente en el documento COBIT menciona:" Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas."

La Normativa "Confiabilidad" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente."

2.3.9.2. CONDICIÓN:

Al efectuar la revisión de la seguridad para el área de T.I. del SFE, se determinó que no existe un estudio de penetración contratado a una empresa especializada en ese tipo de consultarías, el cual podría mostrar ciertas debilidades en el área de telecomunicaciones.

2.3.9.3. CAUSA:

No se han tomado las medidas necesarias para poder implementar un estudio de penetración en el área de tecnologías de información del SFE.

2.3.9.4. EFECTO:

Al no tener identificadas las debilidades que podrían aparecer en un estudio de penetración se corre el riesgo de que la información almacenada en los sistemas de información del SFE sea dañada o filtrada afectando la operatibilidad de la organización.

2.3.9.5. RECOMENDACIÓN:

2.3.9.5.1. Realizar un estudio de penetración de la red de comunicaciones para monitorear las debilidades detectadas en dicho estudio; procediendo a identificar e implantar acciones de mejoramiento, así como un plan de pruebas para valorar las acciones de mejoramiento impulsadas por las actividades de monitoreo y establecer el porcentaje de riesgos corregidos. Este estudio debe ser realizado por una empresa especializada en ese tipo de consultarías, por lo que se requiere el apoyo de la administración para asignar los recursos requeridos para la contratación de dicho servicio.

2.3.10. OBSERVACIÓN 10: NO SE RESPALDA LA INFORMACIÓN CRÍTICA DE USUARIOS FINALES.

2.3.10.1. CRITERIO:

La Normativa "Seguridad en las Operaciones y Comunicaciones" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)"de la Contraloría General de la República, menciona: "La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar el riesgo de fallas y proteger la integridad del software y de la información.

Para ello debe:

a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicios" o virus."

La Normativa "Seguridad" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."

2.3.10.2. CONDICIÓN:

Actualmente las áreas usuarias (laboratorios de control de calidad, planillas, contabilidad, financiero) llevan el control de varios procesos (estadísticas, liquidaciones, proceso contable, etc.) en hojas electrónicas o documentos de Word; sin embargo, esta información en la mayoría de los casos sólo se respalda en las máquinas de los usuarios.

2.3.10.3. CAUSA:

Ausencia de procedimientos en el SFE sobre el tratamiento de la información que se maneja en archivos electrónicos (Word, Excel).

2.3.10.4. EFECTO:

Al llevar el control de procesos en archivos electrónicos se corren riesgos como:

- Control de cambios: no se mantiene un proceso controlado de los requerimientos de cambios. Se debe obtener una aprobación formal de un empleado.

- Control de versión: Se debe asegurar que la versión actual aprobada del archivo de trabajo se usa mediante estándares.

- Controles de acceso: (ejemplo: crear, leer, actualizar y borrar): se corre el riesgo de que el acceso a los archivos no sea restringido, por lo que se deben tener contraseñas para restringir el acceso.

- Controles de entrada: No se asegura que existan reconciliación para que los datos ingresados estén completos y sean adecuados. Los datos pueden ser ingresados a los archivos de trabajo manual o sistemáticamente por medio de descargas de información, por lo que deben existir los mecanismos de control adecuados.

- Seguridad e Integridad de los datos: Se debe implementar un proceso para asegurar que los datos contenidos en los archivos de trabajo sean actuales y seguros, esto puede realizarse protegiendo celdas para impedir cambios inadvertidos o intencionales en los datos (Excel). Además los archivos de trabajo deben estar almacenados en directorios protegidos.

- Documentación: Se debe garantizar que la documentación del archivo de trabajo sea la adecuada y que se mantenga actualizada para que facilite el entendimiento de los procesos.

- Respaldo: se debe implementar un proceso de respaldo periódico del archivo de trabajo para que la información este completa y disponible.

- Archivos: Se deben mantener archivos históricos para que no sea posible actualizarlos ni ponerlos como "Solo Lectura"

- Inspección lógica: Se deben realizar inspecciones lógicas por otro empleado ajeno al creador del archivo de trabajo. Esta revisión debe ser documentada.

- Falta de pistas de auditoría o bitácoras.

2.3.10.5. RECOMENDACIONES:

2.3.10.5.1. Elaborar, aprobar, divulgar e implementar procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

2.3.10.5.2. Realizar respaldos periódicos en un servidor, de la información crítica de uso laboral de las distintas unidades del SFE.

2.3.10.5.3. Mantener copias de seguridad de los respaldos realizados como producto de la recomendación 2.3.10.5.2, y verificar el adecuado respaldo de esos datos.

2.4. DEBILIDADES EN TECNOLOGÍAS

2.4.1. OBSERVACIÓN 1: NO SE CUENTA CON UNA HERRAMIENTA AUTOMATIZADA PARA EL CONTROL DE VERSIONES

2.4.1.1. CRITERIO:

La Normativa "Implementación de infraestructura tecnológica" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)"de la Contraloría General de la República, menciona: "La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos."

REFERENCIA A COBIT	*AI 3 Adquirir y mantener la infraestructura tecnológica*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Plan de adquisición de infraestructura tecnológica. • Protección y disponibilidad del recurso de infraestructura. • Mantenimiento de la infraestructura. • Ambiente de prueba de factibilidad.

2.4.1.2. CONDICIÓN:

Al efectuar la revisión de la implementación de software, se determinó que el área de Análisis y Diseño de Sistemas no cuenta con una herramienta automatizada para controlar las versiones de las distintas aplicaciones en desarrollo.

2.4.1.3. CAUSA:

La Sección de Informática no ha implementado la herramienta de control de versiones denominada "Sourcesafe", la cual forma parte de Microsoft Visual Studio, lenguaje de programación utilizado para el desarrollo de sistemas en el SFE.

2.4.1.4. EFECTO:

No se cuenta con un mecanismo de almacenaje automatizado de los elementos que se deben gestionar (ej. archivos de texto, imágenes, documentación, ejecutables...) en el desarrollo de aplicaciones. Por otra parte no se controlan los cambios a modificaciones parciales, al código fuente, ni se cuenta con un registro histórico de las acciones realizadas con cada elemento que intervienen en el desarrollo de sistemas.

2.4.1.5. RECOMENDACIÓN:

2.4.1.5.1. Implementar la herramienta de control de versiones denominada "Sourcesafe", la cual forma parte de Microsoft Visual Studio, lenguaje de programación utilizado para el desarrollo de sistemas en el SFE.

2.4.2. OBSERVACIÓN 2: NO SE CUENTA CON PLANES DE PRUEBAS PARA LOS RESPALDOS DE LA INFORMACIÓN.

2.4.2.1. CRITERIO:

La Normativa "Administración de los datos" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura."

REFERENCIA A COBIT	*DS 11 Administrar los datos*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Requerimientos del negocio para administración de datos. • Acuerdos de almacenamiento y conservación. • Sistema de administración de librerías de medios. • Eliminación. • Respaldo y restauración. • Requerimientos de seguridad para la administración de datos.

La Normativa "Confiabilidad" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente."

2.4.2.2. CONDICIÓN:

La Sección de Informática cuenta actualmente con un procedimiento para el respaldo de la información almacenada en los servidores; sin embargo, no se establecen los lineamientos necesarios para poder determinar la integridad de los datos almacenados.

2.4.2.3. CAUSA:

No se cuenta con un procedimiento para valorar la integridad de la información respaldada.

2.4.2.4. EFECTO:

Se corre el riesgo de que la información respaldada tenga errores, lo cual no permitiría su utilización en una contingencia.

2.4.2.5. RECOMENDACIÓN:

2.4.2.5.1. Elaborar, aprobar, divulgar e implementar un procedimiento de prueba de los respaldos de la información a un nivel detallado y que contemplen entre otros los factores siguientes:

- Definición del procedimiento para realizar las pruebas a los respaldos.
- Política formal que especifique la periodicidad para realizar las pruebas.
- Definición de políticas y procedimientos relacionados con la vida útil de los medios utilizados para almacenar los respaldos.
- Procedimientos detallados para la clasificación de las cintas y control de inventarios.
- Requerimientos ambientales y técnicos para el almacenamiento de los respaldos y las respectivas pruebas.
- Administración de la capacidad de los medios físicos utilizados para el respaldo y las pruebas.
- Identificación clara del software, aplicaciones y datos a probar.

2.4.3. OBSERVACIÓN 3: FALTANTE DE LICENCIAS DE SOFTWARE.

2.4.3.1. CRITERIO:

La Normativa "Implementación de software" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos."

2.4.3.2. CONDICIÓN:

Al efectuar la revisión sobre la implementación de software, se determinó que el SFE tiene un déficit de licencias en algunos de los programas que seguidamente se detallan.

VERSIONES DE OFFICE	Número de Instalaciones	Total de Licencias	Faltante y/o Sobrante
- Microsoft Office 2000 Professional	12	10	-2
- Microsoft Office 2003 Small Business	1	0	-1
- Microsoft Office 2003 Profesional	152	0	-152
- Microsoft Office 2007 Basic	15	0	-15
- Microsoft Office 2007 Standard	11	0	-11
- Microsoft Office 2007 Profesional	34	0	-34
- Microsoft Office 2007 Enterprise	5	0	-5
SISTEMAS OPERATIVOS PC's	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Windows XP Profesional	195	169	-26
- Windows Vista Home Basic	1	0	-1
DATABASE	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft SQL Server 2000 Standard	1	0	-1
- Microsoft SQL Server 2005 Standard	1	0	-1

APLICACIONES MICROSOFT EN PC`s	Número de Instalaciones	Total de Licencias	Faltante y/o Sobrante
- Microsoft Project 2000	2	0	-2
- Microsoft Project 2003 Profesional	1	0	-1
- Microsoft Project 2007 Profesional	2	0	-2
- Microsoft Visio 2000	2	0	-2
- Microsoft Visio 2007 Profesional	1	0	-1
- Microsoft One Notes 2003	1	0	-1
- Microsoft Virtual Pc 2004	1	0	-1
HERRAMIENTAS DESARROLLO	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft Visual Studio 6.0 Profesional	1	0	-1
- Microsoft Visual Studio 6.0 Enterprise	3	0	-3
- Microsoft Visual Studio 2005 Profesional	4	0	-4
VERSIONES DE OFFICE	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft Office 2003 Profesional	1	0	-1
SISTEMAS OPERATIVOS Servidores	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Windows 2003 Server Standard	8	7	-1
- Windows 2003 Server Enterprise	5	1	-4
MOTORES DE BASES DE DATOS	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft SQL Server 2000 Standard	7	0	-7
APLICACIONES MICROSOFT EN Servidores	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft ISA Server 2006	1	0	-1

CLIENT ACCESS WINDOWS	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Windows 2003 Server Enterprise CAL	591	150	-441
CLIENT ACCESS MAIL	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft Exchange Server 2003 Standard CAL	657	150	-507
CLIENT ACCESS DATABASE	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
HERRAMIENTAS DESARROLLO	**Número de Instalaciones**	**Total de Licencias**	**Faltante y/o Sobrante**
- Microsoft Visual Studio 2005 Premier	1	0	-1

Además, cabe mencionar que la Ley de Protección Fitosanitaria N° 7664, en su artículo N° 64 establece que "Los recursos que se obtengan por lo establecido en el artículo 63 y el Transitorio I, serán utilizados para el cumplimiento de los objetivos de esta Ley y para fortalecer, desarrollar, actualizar y mejorar los servicios que el Servicio Fitosanitario del Estado presta". Asimismo, su artículo 65 señala que "Lo recaudado por la ejecución de la presente Ley se destinará, exclusivamente, a la operación normal del Servicio Fitosanitario del Estado …". En ese sentido, la Contraloría General de la República ha sido reiterativa en indicar que efectivamente lo recaudado por la citada Ley, será utilizado exclusivamente para cumplir su cumplimiento. Cabe mencionar que actualmente el SENASA utiliza licencias de correo electrónico del SFE ya que carece de la cantidad de cuentas de correo necesarias para dotar a todos sus empleados de las mismas.

2.4.3.3. CAUSA:

No se cuenta con la cantidad de licencias suficientes en algunas de las aplicaciones instaladas en el SFE.

2.4.3.4. EFECTO:

Se podría involucrar al SFE en problemas de licenciamiento ante el Registro Nacional de Derechos de Autor ya que la Institución sigue utilizando los programas con licencias faltantes, lo cual se da especialmente con las cuentas de correo de SENASA. Dicho aspecto eventualmente podría generar responsabilidades para los funcionarios que por acción u omisión permiten que esta situación se mantenga.

2.4.3.5. RECOMENDACIONES:

2.4.3.5.1. Suprimir el uso de software que no está soportado en licencias debidamente adquiridas; individualizando las que están siendo utilizadas por el SFE de las del SENASA. Las medidas que adopte la administración activa deberán quedar debidamente documentadas.

2.4.3.5.2. Destinar los recursos necesarios para la adquisición de las licencias faltantes que requiere el SFE (incluye la adquisición de licencias corporativas). Al respecto, se debe adoptar las medidas necesarias, con relación al software que está siendo utilizado por dependencias del SFE sin contar con las licencias respectivas. Las medidas que adopte la administración activa deben quedar debidamente documentadas.

2.4.4. OBSERVACIÓN 4: NO ESTA DOCUMENTADA LA METODOLOGÍA PARA LA ADMINISTRACIÓN DE PROYECTOS INFORMÁTICOS

2.4.4.1. CRITERIO:

La Normativa "Gestión de Proyectos" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, indica: "La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos."

REFERENCIA A COBIT	PO 10 Administrar proyectos
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Marco de trabajo para la administración de programas y proyectos. • Enfoque de administración de proyectos. • Compromiso de los interesados. • Estatuto de alcance del proyecto. • Inicio de las fases del proyecto. • Plan integrado del proyecto. • Recursos del proyecto. • Administración de riesgos del proyecto. • Plan de calidad del proyecto. • Control de cambios del proyecto. • Planeación del proyecto y métodos de aseguramiento. • Medición del desempeño, reportes y monitoreo del proyecto. • Cierre del proyecto.

La Normativa "Gestión de proyectos" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la Institución emprenda, incluyendo los proyectos de obra pública relativos a construcciones nuevas o al mejoramiento, adición, rehabilitación o reconstrucción de las ya existentes.

Las actividades de control que se adopten para tales efectos deben contemplar al menos los siguientes asuntos:

a. La identificación de cada proyecto, con indicación de su nombre, sus objetivos y metas, recursos y las fechas de inicio y de terminación.

b. La designación de un responsable del proyecto con competencias idóneas para que ejecute las labores de planear, organizar, dirigir, controlar y documentar el proyecto.

c. La planificación, la supervisión y el control de avance del proyecto, considerando los costos financieros y los recursos utilizados, de lo cual debe informarse en los reportes periódicos correspondientes. Asimismo, la definición de las consecuencias de eventuales desviaciones, y la ejecución de las acciones pertinentes.

d. El establecimiento de un sistema de información confiable, oportuno, relevante y competente para dar seguimiento al proyecto.

e. La evaluación posterior, para analizar la efectividad del proyecto y retroalimentar esfuerzos futuros."

2.4.4.2. CONDICIÓN:

No se ha documentado el marco para el control de proyectos de TI, que contemple metodologías, planes, procesos de administración de riesgos, aseguramiento de la calidad entre otros aspectos que involucran la eficiente administración de proyectos tecnológicos.

2.4.4.3. CAUSA:

El SFE no ha realizado las gestiones necesarias para contar con una metodología para la administración de proyectos informáticos.

2.4.4.4. EFECTO:

No se asegura la adecuada administración de los proyectos informáticos ni el debido seguimiento al ciclo de vida de los sistemas computacionales (factibilidad, diseño, producción, culminación y puesta en marcha) ni a las respectivas fases (conceptual, definición, adquisición o producción, operación y finalización), ya que actualmente el desarrollo de sistemas de información eficaces requiere de una administración adecuada, que garantice una orientación acorde con los objetivos y estrategias de la organización, dentro de las limitaciones de recursos y de tiempo.

2.4.4.5. RECOMENDACIÓN:

2.4.4.5.1. Elaborar, aprobar, divulgar e implementar la metodología para la administración de proyectos informáticos llevados a cabo en el SFE. Dicha metodología debe definir claramente las etapas del proyecto, la conformación y administración del equipo de trabajo, herramientas utilizadas (por ejemplo diagramas de hitos, Gantt, etc, técnicas utilizadas por ejemplo PERT, modelos de estimación empleados, entre otros aspectos relevantes para la adecuada administración de proyectos informáticos).

2.4.5. OBSERVACIÓN 5: NO SE CUENTA CON UNA METODOLOGÍA PARA EL DESARROLLO DE SISTEMAS.

2.4.5.1. CRITERIO:

La Normativa "Implementación de software" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.

b. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.

c. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.

d. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.

e. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento."

2.4.5.2. CONDICIÓN:

Se determinó que la Sección de Informática del SFE no cuenta actualmente con una metodología formal para el desarrollo de sistemas y mantenimiento de sistemas de información, la cual asegure el éxito y calidad de los proyectos a desarrollar.

2.4.5.3. CAUSA:

La gestión del SFE no ha sido suficiente para poder contar con la metodología requerida.

2.4.5.4. EFECTO:

No se garantiza controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración, de una forma adecuada y estandarizada.

2.4.5.5. RECOMENDACIÓN:

2.4.5.5.1. Elaborar, aprobar, divulgar e implementar una metodología formal de desarrollo y mantenimiento de sistemas, que contemple entre otros factores los siguientes:

- Diseños de alto y bajo nivel.
- Control y auditabilidad de las aplicaciones.
- Seguridad y disponibilidad de las aplicaciones.
- Configuración e implementación del software desarrollado.
- Actualizaciones en los sistemas en producción.
- Aseguramiento de la calidad del software.
- Administración de los requerimientos de aplicaciones.
- Administración de cambios en la plataforma tecnológica.
- Control de versiones de los códigos fuentes.
- Controles cruzados y división de funciones en las labores de:
    - Análisis, diseño, desarrollo e implementación

2.4.6. OBSERVACIÓN 6: CARENCIA DE ESTUDIOS DE FACTIBILIDAD PARA PROYECTOS TECNOLÓGICOS.

2.4.6.1. CRITERIO:

Es importante que la sección de informática cuente con un documento de factibilidad de proyectos tecnológicos en donde se expongan condiciones tales como:

Factibilidad Económica: La factibilidad económica, está definida en función de la capacidad presupuestaria que presenta la Institución en un momento determinado.

Factibilidad Operativa: Que la Sección de Informática cuente con el recurso humano suficiente y capacitado para supervisar una labor en específico.

Factibilidad Técnica: Desde el punto de vista técnico, es rescatable el hecho de que la propuesta responda de manera directa a las estrategias esbozadas en los correspondientes Planes Estratégicos u Operativos.

2.4.6.2. CONDICIÓN:

Al momento de realizar nuestra visita para efectuar la revisión de la "Gestión de Recursos Informáticos", se determinó la ausencia de documentos en donde se notara un estudio de factibilidad de los diversos proyectos tecnológicos a desarrollar mediante contrato o desarrollados por la Sección de Informática del SFE.

2.4.6.3. CAUSA:

No existen manuales o documentación sobre los pasos a seguir para realizar los estudios de factibilidad de los proyectos tecnológicos por parte de la Sección de Informática del SFE.

2.4.6.4. EFECTO:

Si estos estudios no son utilizados en futuros proyectos, no se tendrá la posibilidad de analizar las mejores alternativas presentes y determinar si un proyecto es viable en los aspectos técnicos, operativos y económicos.

2.4.6.5. RECOMENDACIÓN:

2.4.6.5.1. Implementar estudios de factibilidad técnica, económica y operacional de todo nuevo proyecto de tecnologías de información que se desee implementar en el SFE.

2.4.7. OBSERVACIÓN 7: INCUMPLIMIENTO DE LOS ESTÁNDARES DEFINIDOS PARA LA ADMINISTRACIÓN DE BASES DE DATOS.

2.4.7.1. CRITERIO:

La Normativa "Implementación de software" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona: "La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos".

2.4.7.2. CONDICIÓN:

Al efectuar la revisión de la documentación de los estándares que deben estar implantados en las "Bases de Datos" (DB) del SFE, se determinó que los mismos no se están cumpliendo. El estándar de BD menciona:

> *"…Siempre deberá existir un análisis de la base de datos antes de la implantación de cualquier Base de Datos o sus partes constituyentes y deberá contar, tanto en forma impresa como electrónica, al menos con los siguientes elementos:*
>
> *1º. Diagrama de Clases.*
>
> *2º. Diagrama entidad relación, con todas las tablas, llaves y las relaciones correspondientes.*
>
> *3º. Para cada procedimiento almacenado o función que vaya más allá de un select, insert, update o delete, ó que afecte a dos o más tablas, debe existir un diagrama de actividad.*
>
> *4º. En los casos en los que una vista, procedimiento o función utilice o se relacione con cualquier otro objeto en la base de datos distinto a tablas, deberá realizarse un diagrama de colaboración de dicha relación, haciendo mención de los parámetros enviados y recibidos, y los tipos de datos de dichos parámetros, de tal manera que el DBA pueda determinar con solo ver este diagrama que otros componentes de la base de datos se ven afectados al modificar o eliminar una objeto determinado.*

Se recomienda que los puntos 3º y 4º se adjunten a la documentación una vez concluida la fase de desarrollo del sistema.

En el momento en que cualquier cambio a los objetos de las bases de datos modificara cualquiera de los diagramas mencionados, estos deberán ser actualizados inmediatamente.

Con este se busca estandarizar aspectos relevantes de los objetos como el uso de nombres, documentación, seguridad, y rendimiento. La implementación de los estándares en este manual es de seguimiento obligatorio para todas las Bases de Datos del Ministerio. [8] "

Sin embargo de la revisión realizada, se determinó que no se ha implementado dicho estándar. Al respecto, únicamente se cuenta con un "diagrama entidad relación"[9].

2.4.7.3. CAUSA:

Incumplimiento de estándares establecidos por la misma Sección de Informática del SFE, situación que se genera aparentemente por la falta de personal, aspecto que ha dificultado la implementación de esos estándares de bases de datos como diagramas de clases, diagramas de actividad y diccionario de datos.

2.4.7.4. EFECTO:

Al no existir una estandarización en la documentación de las bases de datos se hace muy difícil la labor de mantenimiento y mejoras que se deben hacer para mejorar los servicios que se brindan a través de los sistemas automatizados.

2.4.7.5. RECOMENDACIÓN:

2.4.7.5.1. Implementar los estándares internos de bases de datos desarrollados por la Sección de Informática del SFE, para poder unificar la arquitectura de las bases de datos y facilitar el mantenimiento de las mismas.

[8] Documento Estándares DBA, área análisis y diseño de sistemas SFE
[9] Un **diagrama o modelo entidad-relación** (a veces denominado por su siglas, *E-R* "Entity relationship", o, "DER" Diagrama de Entidad Relación) es una herramienta para el modelado de datos de un sistema de información. Estos modelos expresan entidades relevantes para un sistema de información así como sus interrelaciones y propiedades.

2.4.8. OBSERVACIÓN 8: AUSENCIA DE UN PLAN FORMAL DE ADMINISTRACIÓN DE LA CAPACIDAD Y DESEMPEÑO DE LA PLATAFORMA TECNOLÓGICA

2.4.8.1. CRITERIO

La Normativa "infraestructura tecnológica" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona:" La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI."

REFERENCIA A COBIT	*PO 3 Definir la dirección tecnológica*
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Planeación de la dirección tecnológica. • Plan de infraestructura tecnológica. • Monitoreo de tendencias y regulaciones futuras. • Estándares tecnológicos. • Consejo de arquitectura.

2.4.8.2. CONDICIÓN:

Actualmente no se cuenta con un plan debidamente documentado que permita la administración de la capacidad y desempeño de la plataforma tecnológica del SFE.

2.4.8.3. CAUSA

La gestión del SFE no ha sido suficiente, situación que no permite contar a la fecha con dicho plan.

2.4.8.4. EFECTO

No se cuenta con indicadores reales sobre el rendimiento de la plataforma tecnológica, con el fin de establecer planes de ampliación y mejoramiento futuros.

2.4.8.5. RECOMENDACIÓN:

2.4.8.5.1. Establecer procedimientos y políticas formales para la plataforma tecnológica, los cuales contemplen entre otros los factores siguientes:

- Administración de la capacidad de la plataforma tecnológica:
  - Promedios de tiempos de respuesta.
  - Cantidad de transacciones diarias.
  - Generación de informes.
- Monitoreo de la capacidad de procesamiento de los servidores principales.
- Evaluación periódica del rendimiento de los equipos principales de la plataforma tecnológica.
- Evaluaciones y motivos de la interrupción de los servicios.
- Administración de las operaciones y configuraciones.
- Programación calendarizada de las tareas.
- Monitoreo del crecimiento de la configuración de la plataforma tecnológica.
- Mecanismos de control que garanticen la ausencia de software o hardware no autorizado.
- Asignación de responsabilidad por la administración de la configuración.
- Identificación de los distintos elementos de la configuración de la plataforma tecnológica.

2.5. DEBILIDADES EN LA ADMINISTRACIÓN DE RIESGOS

2.5.1. OBSERVACIÓN 1: NO SE HA DESARROLLADO UNA METODOLOGÍA FORMAL PARA LA ADMINISTRACIÓN DEL RIESGO INFORMÁTICO

2.5.1.1. CRITERIO:

La Normativa "Gestión del riesgo" presente en el documento "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, menciona:" La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."

REFERENCIA A COBIT	PO 9 Evaluar y administrar riesgos de TI
OBJETIVOS ESPECIFICOS DE COBIT RELACIONADOS	• Alineación de la administración de riesgos de TI y del negocio. • Establecimiento del contexto del riesgo. • Identificación de eventos. • Evaluación de riesgos. • Respuesta a los riesgos. • Mantenimiento y monitoreo de un plan de acción de riesgos.

La Normativa "Sistema Específico de Valoración del Riesgo Institucional" presente en el documento "Normas Generales de Control Interno Sector Público (N-2-2009-CO-DFOE)" de la Contraloría General de la República, menciona:" El jerarca y los titulares subordinados, según sus competencias, deben establecer y poner en funcionamiento un Sistema Específico de Valoración del Riesgo Institucional (SEVRI).

El SEVRI debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable. Asimismo, debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento."

2.5.1.2. CONDICIÓN:

Mediante el informe de auditoría comunicado con oficio AI SFE 171-2009 del 05/11/2009, se indicó que la gestión emprendida por el SFE no ha sido suficiente para la implementación del SEVRI.

2.5.1.3. CAUSA:

Poca efectividad en la implementación del SEVRI.

2.5.1.4. EFECTO:

No se tienen identificados los posibles riesgos en materia tecnológica, por lo que ante la materialización de algún riesgo no se cuenta con mecanismos adecuados para mitigar su impacto.

2.5.1.5. RECOMENDACIÓN:

2.5.1.5.1. Adoptar las medidas necesarias que le permitan al SFE ajustar su sistema de control interno relativo a la Sección de Informática del SFE al ordenamiento jurídico y técnico vigente en materia de control interno; gestión que debe permitir el establecimiento del SEVRI vinculado con las tecnologías de información[10]. La implementación de dichas medidas debe ser consistente con la implementación de la recomendación número 2.1.6.1, contenida en el informe de la Auditoría Interna del SFE N° AI-SFE-SA-INF-001-2009, comunicado con oficio Nº AI-SFE-042-2009 de fecha 17/04/2009.

[10] Debe contemplar medidas preventivas como por ejemplo contratos con otros proveedores, mantenimiento preventivo, bitácoras para el acceso a los servidores, etc. También se deben definir los riesgos, clasificarlos, identificarlos (aceptación, eliminación, reducción, transferencia del riesgo); asimismo, se debe analizar el impacto de los riesgos, tomando en cuenta el tiempo de recuperación, la probabilidad que ocurra un riesgo, así como la implementación de planes de entrenamiento y pruebas para el personal.

2.5.2. OBSERVACIÓN 2: NO EXISTEN PÓLIZAS PARA LOS SERVIDORES DEL SFE.

2.5.2.1. CRITERIO:

Los equipos computacionales críticos del SFE como servidores y equipo de comunicaciones deben contar con pólizas lo más detalladas posibles, para que en caso de un siniestro o contingencia se pueda determinar con claridad cuál es el monto que la aseguradora debe rembolsar por la pérdida o daño del equipo asegurado en general o de uno en particular.

2.5.2.2. CONDICIÓN:

Al efectuar la revisión de los seguros computacionales para los equipos críticos como servidores del SFE se determinó que estas pólizas no existen.

2.5.2.3. CAUSA:

El SFE no ha considerado a la fecha la necesidad de contar con este tipo de mecanismo para un eventual resarcimiento.

2.5.2.4. EFECTO:

En caso de un siniestro o contingente que cause daño a algunos de los equipos que se encuentran en el área de servidores no se recuperaría la inversión o parte de la misma.

2.5.2.5. RECOMENDACIÓN:

2.5.2.5.1. Valorar la posibilidad de dotar al equipo computacional crítico como servidores del SFE de un seguro, que cubra la inversión realizada en forma parcial o total, es conveniente se especifique el equipo asegurado y el monto del seguro. La decisión que se adopte debe fundamentarse y documentarse.

III. CONCLUSIONES GENERALES

En nuestra opinión, encontramos la Gestión de Tecnologías de Información del SFE en disconformidad con las normas técnicas aplicables al sector público.

Hemos identificado oportunidades para mejorar los controles de la Sección de Informática del SFE, con respecto a la Gestión de Tecnologías de Información, según lo discutido en este informe.

Como cierre de esta sección se establece un resumen del cumplimiento de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, por parte de la Institución:

Marco estratégico de TI

NORMA ESTABLECIDA	*DESARROLLO INICIAL*	*AVANCE INTERMEDIO*	*CUMPLIMIENTO TOTAL*
Marco estratégico de TI	X		
Gestión de la calidad	X		
Gestión de riesgos	X		
Gestión de la seguridad de la información		X	
Implementación de un marco de seguridad de la información		X	
Compromiso del personal con la seguridad de la información		X	
Seguridad física y ambiental	X		
Seguridad en las operaciones y comunicaciones		X	
Control de acceso		X	
Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica		X	
Continuidad de los servicios de TI	X		
Gestión de proyectos	X		
Decisiones sobre asuntos estratégicos de TI	X		
Cumplimiento de obligaciones relacionadas con la gestión de TI	X		

Planificación y organización

NORMA ESTABLECIDA	*DESARROLLO INICIAL*	*AVANCE INTERMEDIO*	*CUMPLIMIENTO TOTAL*
Planificación de las tecnologías de información	X		
Modelo de arquitectura de información		X	
Infraestructura tecnológica		X	
Independencia y recurso humano de la Función de TI		X	
Administración de recursos financieros		X	

Implementación de tecnologías de información

NORMA ESTABLECIDA	*DESARROLLO INICIAL*	*AVANCE INTERMEDIO*	*CUMPLIMIENTO TOTAL*
Consideraciones generales de la implementación de TI		X	
Implementación de software	X		
Implementación de infraestructura tecnológica		X	
Contratación de terceros para la implementación y mantenimiento de software e infraestructura		X	

Prestación de servicios y mantenimiento

NORMA ESTABLECIDA	*DESARROLLO INICIAL*	*AVANCE INTERMEDIO*	*CUMPLIMIENTO TOTAL*
Definición y administración de acuerdos de servicio		X	
Administración y operación de la plataforma tecnológica	X		
Administración de los datos		X	
Atención de requerimientos de los usuarios de TI		X	
Manejo de incidentes		X	
Administración de servicios prestados por terceros		X	

Seguimiento

NORMA ESTABLECIDA	*DESARROLLO INICIAL*	*AVANCE INTERMEDIO*	*CUMPLIMIENTO TOTAL*
Seguimiento de los procesos de TI		X	
Seguimiento y evaluación del control interno en TI	X		
Participación de la Auditoría Interna		X	

IV. SEGUIMIENTO A AUDITORIAS ANTERIORES

Mediante el oficio AI 307-2003 del 19/12/2003 la Auditoría Interna del MAG remitió a la administración activa los informes con los resultados de estudios de auditoría interna relativos a la evaluación del control interno en tecnologías de información que se llevó a cabo en el SFE. Los informes citados son los siguientes:

a) Resultados del estudio de auditoría relativo a la evaluación del sistema de recaudación de ingresos (RECAUDA) del Servicio Fitosanitario del Estado.
b) Resultados del estudio de auditoría relativo a la evaluación del Sistema de PRESUPUESTO (SIEP) del Servicio Fitosanitario del Estado.
c) Resultados del estudio de auditoría relativo a la evaluación del Sistema de combustibles del Servicio Fitosanitario del Estado.
d) Resultados del estudio de auditoría relativo a la evaluación del proceso de adquisición, desarrollo y mantenimiento de sistemas del Servicio Fitosanitario del Estado.
e) Resultados del estudio de auditoría relativo a la evaluación del Sistema de inventarios del Servicio Fitosanitario del Estado.
f) Resultados del estudio de auditoría relativo a la evaluación del sistema de recaudación de ingresos (SACI) del Servicio Fitosanitario del Estado.
g) Oficio sin número de fecha 17 de diciembre del 2003 con las recomendaciones generales aplicables a todos los sistemas evaluados

Con base en la evidencia obtenida, se determinó que las recomendaciones contenidas en los informes que se describen en los incisos a), b) y c) perdieron vigencia, por cuanto dichos sistemas no se encuentran en producción.

4.1. ESTADOS DE LAS RECOMENDACIONES SUJETAS A SEGUIMIENTO

Se procede a describir el estado de las recomendaciones (situación al 23/11/2009) consignadas en los informes citados en los incisos d), e) y f) anteriores. Al respecto, el estado de las recomendaciones se identificará con las siguientes siglas:

- RC = Recomendación Cumplida.
- RPC = Recomendación en Proceso.
- RNC = Recomendación no Cumplida.
- RNV = Recomendación no Vigente.

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Planeación estratégica y control de proyectos de desarrollo. Condición: El Servicio Fitosanitario no cuenta con elementos básicos de planeación, organización y control del proceso de desarrollo y mantenimiento de sistemas, entre ellos un plan estratégico informático que contemple proyectos por llevar a cabo, un plan anual de trabajo, un presupuesto ni mecanismos para el control de proyectos de desarrollo ni métricas de productividad del personal en esa área.	1. Trabajar en la elaboración de un plan estratégico informático que dicte en rumbo en materia de desarrollo y mantenimiento de sistemas y que contemple al menos los siguientes aspectos: estrategia de desarrollo y mantenimiento por seguir (interno, externo, combinado), establecimiento de un modelo de datos organizacional, plataforma tecnológica, necesidades de herramientas, necesidades de capacitación, proyectos de desarrollo identificados.	*Desconozco si en su momento se hizo este plan estratégico ya que nunca recibí ningún tipo de información ni un informe de labores cuando asumí la jefatura de la Sección de Informática.*	**RNC** Con lo que se cuenta es con un POI para el área de T.I. y a nivel institucional
Documentación de contratación de sistemas con fondos de OIRSA. Condición: No se pudo verificar el cumplimiento de los términos contractuales ni analizar el proceso de contratación de los sistemas desarrollados con fondos del organismo internacional OIRSA (Inventarios, sistema de control de ingresos y presupuesto) debido a la imposibilidad de acceso a la documentación de estos desarrollos.	2. Definir y oficializar normativa y procedimientos básicos relativos al área de adquisición, desarrollo y mantenimiento de sistemas, entre ellos: a. Metodología para el desarrollo y mantenimiento de sistema. b. Procedimientos para la contratación externa de desarrollos o mantenimientos. c. Procedimiento para pases a producción de los sistemas. d. Procedimiento para el control de versiones de los sistemas en las estaciones		**RNC**

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	d. Procedimiento para la solicitud de cambios en los sistemas. e. Procedimientos de administración y respaldo de programas fuente. f. Estándares de diseño de la interfase con el usuario. h. Estándares de pruebas y aceptación de sistemas.		
Expedientes de cada proyecto de desarrollo Condición: No se manejan a nivel del área informática ni de los usuarios responsables de los sistemas en desarrollo un expediente por cada sistema que incluyan los documentos básicos que permitan documentar el proceso de desarrollo.	3. Girar instrucciones a la Gerencia Administrativa y Financiera en el sentido de mantener un expediente completo y ordenado de cada proceso de contratación de desarrollo de sistemas, sea financiado con recursos del Servicio Fitosanitario o con recursos de donaciones.		**RC**
Participación de contraparte técnica en desarrollo. Condición: No se ha tenido una participación activa del personal de cómputo en el proceso de desarrollo del sistema de presupuesto, que en la actualidad está en fase de pruebas.	4. Instruir a la Gerencia Administrativa y Financiera en el sentido de que cuando se formalicen contratos para el desarrollo de sistemas, en las cláusulas de forma de pago se estipulen desembolsos contra productos debidamente revisados y aceptados por el Servicio Fitosanitario.		**RNV**

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Aprobación y revisión de productos por parte del usuario Condición: De las entrevistas realizadas a usuarios se desprende que el usuario participa a lo largo del proceso de desarrollo, sin embargo, no se documenta oficialmente su actividad por medio de aprobación de productos ni mecanismos que reflejen una participación activa a lo largo del proceso y su responsabilidad en el Vo.Bo., para el giro de pagos y aceptación de productos.	5. Conformar, cada vez que se inicie un desarrollo, un grupo de trabajo por proyecto, que contemple participación del usuario y personal informático y que se definan formalmente las responsabilidades y roles de cada uno, entre otras: aprobación formal de documentos, de productos, responsabilidades en la aprobación de pagos, administración del archivo o legajo del proyecto con toda la documentación que se ha generado durante su desarrollo (minutas de reuniones, documentos de trabajo, documentos aprobados, documentos de observaciones y acuerdos, entre otros).	Actualmente se realiza, por cuanto se da participación al usuario	**RPC** No se cuenta con aprobaciones de cambio documentadas actualmente, sin embargo, cada vez que se realiza un cambio a un sistema se envía un oficio indicando que el cambio fue realizado satisfactoriamente. Por otra parte existe un procedimiento para mejorar los sistemas de información.
Pagos contra productos terminados y aprobados. Condición: En el desarrollo de las aplicaciones contratadas con fondos de OIRSA no se establecieron esquemas de pagos en función de productos terminados.	6. Preparar y aplicar para los sistemas de presupuesto (SIEP), control de ingresos (SACI), Combustibles, así como los desarrollados por los estudiantes del Tecnológico (Cuarentena y Biblioteca Virtual) un plan formal de pruebas y de aceptación del sistema de tal forma que antes de iniciar su operativa oficial o el proceso de paralelo (cuando aplique) se hayan realizado pruebas completas de funcionalidad.		**RNV** Los sistemas de presupuesto y combustibles no se encuentran en producción y para los otros sistemas mencionados el paralelo o puesta en producción se llevo a cabo hace más de 6 años.

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Procesos de paralelo. Condición: Desde setiembre-2003 se está ejecutando una especie de proceso parcial de paralelo del sistema de recaudación de ingresos con el sistema actual en fox, específicamente el proceso de facturación, sin que se haya definido a la fecha una estrategia formal para realizar un paralelo integral que abarque todas las funcionalidades de la aplicación y contemple cuáles son los mecanismos para conciliar los resultados en ambas aplicaciones (cuadres) y ajustes necesarios para corregir diferencias.	7. Preparar, antes del inicio oficial de operaciones, un plan formal de puesta en marcha de los sistemas que aún no han iniciado operaciones (Combustibles, Control de ingresos, Presupuesto, Cuarentena Biblioteca Virtual), que contemple los siguientes elementos: cronogramas propuestos, recursos humanos requeridos, personal involucrado, roles y responsabilidades, informes).	El sistema en fox ya no existe, desconozco si en su momento se hizo lo solicitado por la Auditoria.	**RNV** Los sistemas que menciona la recomendación ya no se encuentra en producción.
Puesta en marcha del sistema de combustibles y plan de pruebas de aceptación por parte del usuario. Condición: No se ha definido un plan de puesta en marcha del sistema de combustibles ni tampoco hay evidencia de que se haya preparado y ejecutado un plan de pruebas de aceptación por parte del área usuaria.	8. Implementar un ambiente exclusivo para la prueba y mantenimiento de sistemas.		**RNV** El sistema de combustibles no se encuentra en producción.

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Normativa para el desarrollo y mantenimiento de sistemas. Condición: Se carece de normativa básica relacionada con el desarrollo y mantenimiento de aplicaciones. Es así como no existe una metodología oficial para el desarrollo de sistemas que aplique tanto a desarrollos internos como externos, procedimientos para la administración y el control de los programas fuentes y control de versiones de los sistemas. Tampoco hay estándar es en el diseño de interfase usuario-máquina.	9. Gestionar la compra de las licencias de las herramientas de desarrollo faltantes que realmente sean necesarias.		**RNC**
Control de versiones de programas fuente Condición: No se mantiene un adecuado control de versiones de los programas fuente.	10. Restringir el acceso de los analistas a los sistemas en producción de tal forma que se elimine el derecho de modificar o eliminar datos de las bases de datos oficiales.		**RNC**
Formulario de solicitud de mantenimiento de sistemas Condición: Se cuenta con un formulario para la solicitud de mantenimiento de sistemas, cuya utilización inició en octubre de este año, pero no se ha oficializado ni divulgado ningún procedimiento que regule su uso.		No conozco este formulario, actualmente utilizamos un procedimiento para solicitud de cambios y nuevos desarrollos de sistemas.	**RNV** Existe un nuevo formulario vía web
Acceso a programas fuente Condición: Los analistas tienen acceso irrestricto a los programas fuente de los sistemas.		Actualmente si se cuenta con los códigos fuentes de los sistemas en producción.	**RNC**

DESCRIPCIÓN BREVE	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Ambiente para pruebas de sistemas Condición: No existe un adecuado ambiente para pruebas de sistemas que asegure que las versiones que se instalan a los usuarios están debidamente depuradas ni tampoco se da la función de control de calidad.		Se realizan pruebas a los nuevos sistemas, sin embargo no se tiene documentación por escrito de las mismas, esto es algo que estamos implementando actualmente con los nuevos desarrollos, incluyendo los desarrollados por advansys.	**RNC**
Acceso irrestricto de analistas a base de datos en producción Condición: Los analistas de sistemas tienen acceso irrestricto (consulta, modificación y borrado) a la información de las bases de datos de los sistemas en producción que tienen a su cargo.		Actualmente existe un administrador de base de datos que se encarga de administrar los cambios en las bases de datos.	**RC**
Respaldos de programas fuentes Condición: No se cuenta con respaldos actualizados de los programas fuente de las aplicaciones.		Actualmente se cuenta con los respaldos actualizados de los programas fuentes de las aplicaciones desarrolladas internamente por el área de análisis y diseño de sistemas, no podemos responsabilizarnos por aplicaciones que fueron desarrolladas en años anteriores y de las cuales nunca recibimos documentación.	**RC**

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
Inventarios	Acceso a la aplicación Condición: El sistema no cuenta con un mecanismo de acceso que restrinja el acceso a los usuarios.	1. En caso de que la incorporación de un módulo de seguridad al sistema no pueda ser realizada en el corto plazo, instalar una versión reducida del sistema en la estación del funcionario encargado de bodega, de tal forma que solo pueda tener acceso a las opciones típicas del puesto de bodeguero.	Recomendación #1, se creó un módulo de seguridad, en el cual a través de un menú, se le da acceso a los usuarios únicamente a las pantallas que tienen acceso y a su vez, este mismo módulo permite asignar estos permisos, incluso al nivel de actividad a realizar en la pantalla (nuevos registros, modificar, eliminar y consultar). (Recomendación cumplida).	**RC** Se pudo constatar la existencia de cuentas de usuario para el acceso al sistema.
	Inexistencia de perfiles de acceso Condición: Los usuarios de Proveeduría tienen acceso a todos las opciones del sistema.			**RC** Se cuenta actualmente con un modulo de seguridad para otorgar o limitar los accesos al sistema por parte de los usuarios.
	Rastro de las transacciones A Condición El sistema no registra cuál fue el usuario que generó una transacción, en qué fecha ni la hora.	2. Hacer los ajustes necesarios en el diseño de la base de datos y en la programación del sistema de tal forma que puedan ser registrados datos básicos que permitan poder tener el rastro de una transacción: código de usuario, fecha y hora.	Recomendación #2, se modificó el código de la aplicación para que al realizarse una actualización o un borrado en cualquiera de las pantallas, proceda a registrar dentro de la bd's el usuario de sistema, usuario de red, nombre del equipo, fecha, hora y la acción que se efectuó. (Recomendación cumplida).	**RPC** Actualmente si se está guardando la fecha de emisión de la transacción; sin embargo, es recomendable guardar la hora específica de la transacción

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Formato de los códigos de los catálogos Condición: El sistema permite incluir caracteres alfanuméricos (letras, espacios, caracteres especiales) en los códigos productos, direcciones, unidades, secciones).	3. Agregar controles en el proceso de captura de datos de los catálogos de productos y áreas administrativas para que el código digitado por el usuario sea validado como un código numérico (no permita espacios, letras ni caracteres especiales) y que tenga una longitud mínima para lograr uniformidad en los valores asignados y adecuados ordenamientos en los reportes y consultas de estos ítems.	Valorado Nuevo Sistema (SICIC)	**RC** Se cuenta con validaciones para evitar el ingreso de caracteres especiales, letras o espacios.
	Descripción duplicada en catálogos Condición: El sistema permite la inclusión de items de los catálogos (productos, proveedores, dependencias administrativas, bodegas) con la descripción duplicada.			**RNC** No se ha implementado algún control que evite el ingreso de descripciones duplicadas para los catálogos por parte de los usuarios del sistema.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Proveedores con datos en blanco Condición: Se pueden crear proveedores con todos los datos en blanco. El único dato que se graba es el código de proveedor, que es generado automáticamente por el sistema.	4. Incluir en el proceso de mantenimiento de proveedores los siguientes controles: a. Validar que al incluir un proveedor sea requerido como mínimo incluir la cédula, el nombre y un teléfono. b. Establecer un formato estándar para la digitación de la cédula del proveedor c. Validar que al incluir o modificar un proveedor no exista otro con la misma cédula.	Valorado Nuevo Sistema (SICIC)	**RC** Se pudo constatar que se tomaron las previsiones necesarias para evitar guardar proveedores con todos sus campos en blanco. Es deseable que el sistema muestre un mensaje al usuario indicando que se requiere el ingreso de ciertos datos para que la transacción sea guardada de forma exitosa.
	Cédulas de proveedor duplicadas Condición: El sistema permite que se introduzcan varios proveedores con la misma cédula y además en cualquier formato de cédula.			**RNC** No se cuenta con un mecanismo que evite el ingreso de cedulas duplicadas por parte de los usuarios.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Posibilidad de modificar fecha de trámites. Condición: El sistema permite que el usuario digite cualquier valor (inclusive no razonables según la fecha real) en fechas de emisión de solicitudes de compra, requisiciones, órdenes de compra y fecha de inclusión de proveedor, fecha de última compra, fecha de entrega de un producto, entre otras.	5. Modificar el diseño del sistema para incorporar una fecha de proceso para la aplicación que sea utilizada automáticamente para grabar las transacciones de tal forma que los usuarios no puedan manipular la fecha de los trámites y se valide que solo se procesen trámites pertenecientes al periodo presupuestario oficial.	c) Recomendación #5, se imposibilitó a los usuarios modificar tanto las fechas de las solicitudes como de órdenes de compra. (Recomendación cumplida). Valorado Nuevo Sistema (SICIC)	**RNC** No se cuenta con un diseño que evite modificar las fechas de emisión de las solicitudes.
	Posibilidad de digitar valor de "fecha de última compra" de proveedor Condición: Permite digitar el campo de fecha de última compra cuando se incluye un proveedor.	6. Incorporar los siguientes controles en el proceso de mantenimiento de órdenes de compra: a. Validar que si el usuario digita una fecha no válida en el campo de fecha de entrega el sistema así se lo indique mediante un mensaje y evitar que se caiga la aplicación. b. No permitir que se digiten líneas de órdenes de compra con precio 0. c. No permitir eliminar órdenes de compra que tengan líneas con facturas asociadas.	d) Recomendación #6a, se varió la metodología sobre la "fecha de entrega", donde se dan una cantidad específica de días después de la recepción del documento para la entrega. (Recomendación cumplida). e) Recomendación #6b, con respecto a las órdenes de compra, esta debe de estar en la cantidad con un número mayor de uno y el precio debe de ser superior a cero. (Recomendación cumplida). f) Recomendación #6c, por aspectos de integridad referencial en la bd's esto no se permite. (Recomendación cumplida).	**RNC** Aún persiste en el sistema la posibilidad de que el usuario digite la fecha de última compra y el ingreso de un dato no necesariamente valido en formato fecha.

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	Validación de la fecha de entrega de una orden de compra Condición: Cuando se está digitando una nueva orden de compra el sistema se cae si se digitan datos inválidos en el campo de fecha de entrega. Ejemplo: 20/032003 en lugar de 20/03/2003.			**RC** El diseño actual que presenta el sistema evita el ingreso de datos invalidados por parte de los usuarios.
	Solicitudes de compra sin área administrativa asociada. Condición: El sistema permite registrar solicitudes de compra no asociadas a alguna dirección, departamento, unidad o sección.			**RNC** No se cuenta con un control que obligue a los usuarios al ingreso de una dirección, departamento, unidad o sección.
	Órdenes de compra con precios en 0 Condición: Se pueden generar órdenes de compra con el precio de productos en 0.			**RC** Se pudo constatar la existencia de controles que limitan el ingreso de órdenes de compra con precios en cero.
	Herramientas diferentes para selección de elementos de una tabla Condición: No hay uniformidad en la herramienta disponible al usuario para seleccionar items de una lista (de proveedores, productos, áreas). Se tienen dos métodos para hacer lo mismo, uno más ágil que otro.	7. Estandarizar en las pantallas el mecanismo para selección de items de una lista (“grid”). En lo posible utilizar el que proporcione mayor agilidad y ofrezca más funcionalidades para el usuario.		**RC** Actualmente se cuenta con un método para la selección elementos de una tabla, por lo tanto el hallazgo se encuentra subsanado.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Trámites con encabezados y sin líneas de detalle Condición: El sistema permite crear solicitudes de compra, requisiciones y órdenes de compra con solo encabezado, sin líneas de detalle.	8. Incluir en el mantenimiento de requisiciones una validación para no permitir solicitar una cantidad superior a la de existencias de un producto.		**RNC** Actualmente es posible que los usuarios puedan ingresar solicitudes sin líneas de detalle.
	Se pueden eliminar físicamente requisiciones Condición: Se pueden borrar físicamente requisiciones de la base de datos.	9. Realizar modificaciones en la programación de los procesos de mantenimiento de solicitudes de compra, órdenes de compra y requisiciones de tal forma que se asigne el número del trámite y se cree un registro en la base de datos después de haber realizado todas las validaciones de entrada de datos y se hayan incluido las líneas de detalle, con el fin de evitar que se creen encabezados sin líneas asociadas.		**RC** No es posible a través del sistema la eliminación de requisiciones. Es deseable la posibilidad de mostrar un mensaje por pantalla que indique al usuario cuando procede o no la transacción.
	Permite generar requisiciones con cantidades mayor a existencias Condición: Permite emitir requisiciones a pesar de que no haya inventarios en existencia.	10. No permitir en el sistema que se de el borrado físico de órdenes de compra y de requisiciones. En su lugar, se puede implementar el concepto de anulación.		**RNC** Aún es posible registrar en el sistema requisiciones con cantidades mayor a las existentes, sin embargo cabe recalcar que por razones operativas determinaron en el SFE no aplicar cambios en el proceso actual que realiza el

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
				sistema.
	Posibilidad de borrar órdenes de compra después de emitidas. Condición: Una orden de compra se puede modificar o borrar después de haber sido impresa.	11. Incluir en el sistema los controles necesarios para no permitir que se anulen solicitudes de compra que tengan líneas asociadas a órdenes de compra.		**RC** No es posible a través del sistema borrar órdenes de compra, sin embargo es deseable la posibilidad de indicarle al usuario cuando procede o no la transacción, ya que el sistema no muestra ninguna especie de leyenda o mensaje por pantalla.
	Anulación de solicitudes de compra contra mite asociado. Condición: Se pueden eliminar solicitudes de compra que ya tengan líneas asociadas a una orden de compra.	12. Incluir validaciones en los procesos de mantenimiento de los catálogos de productos, proveedores y áreas administrativas de tal forma que no sea posible cambiar su descripción si ya tienen trámites asociados.		**RC** Actualmente se cuenta con controles que impiden el borrado de solicitudes de compra que tengan líneas asociadas a una orden de compra.
	Eliminación física de órdenes de compra con facturas asociadas. Condición: Se pueden eliminar de la base de datos órdenes de compra a pesar de que tengan facturas asociadas	13. Permitir la opción de desactivar productos, proveedores y áreas administrativas de los catálogos, de tal forma que no puedan ser utilizados en nuevos trámites pero que permanezcan en el catálogos para efectos históricos.		**RC** Actualmente se cuenta con controles que impiden el borrado de órdenes de compra que tengan líneas asociadas a una factura por medio del sistema.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Cambio de descripciones de catálogos Condición: Se pueden cambiar descripciones de productos, proveedores y áreas administrativas después de que se han utilizado en órdenes de compra, solicitudes de compra y requisiciones.	14. Valorar la necesidad real de mantener la opción de descuento a nivel del encabezado de orden de compra. Si se requiere, incorporar en el sistema el procedimiento de cálculo respectivo; de lo contrario, eliminar este campo de la pantalla de mantenimiento de órdenes de compra y de la base de datos.		**RC** Actualmente el sistema restringe el cambio de descripciones en catálogos, cabe mencionar que para aplicar una modificación debe ir acompañada mediante nota.
	Desactivación de productos, proveedores o áreas Condición: El sistema no da la posibilidad de desactivar productos, proveedores o áreas administrativas.	15. Eliminar la posibilidad de generar a un formato de archivo modificable el reporte de orden de compra.	h) Recomendación #15, se desactivó la opción de exportación, en ese reporte propiamente, así como también en la consulta de órdenes de compra. (Recomendación cumplida).	**RC** Actualmente es factible mediante el sistema poder desactivar productos, proveedores o áreas administrativas.
	Posibilidad de modificar orden de compra Condición: El reporte de orden de compra se puede generar a un archivo que puede ser modificable.	16. Revisar la programación del reporte de solicitudes por dependencia con el fin de lograr su funcionamiento.	i) Recomendación #16, el reporte es completamente funcional actualmente. (Recomendación cumplida).	**RC** Para solventar el hallazgo se inhabilitó la opción de enviar el reporte a Word, Excel o a algún archivo modificable.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Descuento a nivel del encabezado de la orden de compra Condición: En el reporte de la orden de compra no se calcula el descuento que se digita a nivel del encabezado de la orden de compra.			**RNC** Aún se encuentra pendiente el cálculo correspondiente al descuento que se ingresa en el encabezado de la orden de compra.
	Reporte de solicitudes por dependencia no funciona Condición: El reporte de solicitudes de compra por dependencia no funciona.			**RC** Actualmente se cuenta con un reporte funcional de solicitudes por dependencia.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
SACI	Ambiente en que se corre la aplicación Condición: El usuario tiene instalado un software que permite manipular los datos	1. Desinstalar la herramienta Enterprise Manager de todas las estaciones de los usuarios donde se ubicó y habilitar usuarios con clave a nivel de la base de datos que impidan una conexión directa fácil.	1. Actualmente esta herramienta solo se instala en los servidores del SACI en las regionales, excepto en las estaciones de: Los Chiles y Sixaola, debido a que en las mismas estaciones las bd's están instaladas en una computadora del usuario que utiliza el sistema. Actualmente el Ing. Luis Jiménez ex funcionario del SFE se encuentra realizando la recopilación de requerimientos para desarrollar el sistema SACI en forma web. Lo anterior como parte de su Proyecto Final de Graduación en la UNA. Esta nueva aplicación cumplirá con esta recomendación, a la fecha se está a la espera de que el Ing. Jiménez envié el cronograma del proyecto. Tanto la recomendación Nº 4 y 5 se subsanarán con esta nueva aplicación. (Recomendación en proceso de cumplimiento).	**RPC** Se han realizado las gestiones necesarias de modo que en las estaciones de los usuarios no se tenga instalado este tipo de software, sin embargo actualmente se cuenta con 2 estaciones las cuales aún tienen incorporado el Enterprise Manager
	Intentos fallidos de acceso al sistema Condición: En el sistema de recaudación, se detectan los intentos fallidos y al tercer intento consecutivo la aplicación se cierra. Sin embargo, el usuario puede en forma inmediata volver a intentar el acceso al sistema con lo que	Verificar que las debilidades de control interno que posee el sistema de recaudación actual en FOX sean subsanadas en la implementación del nuevo sistema.	1. Todas las recomendaciones hechas para el sistema de Recaudación de Ingresos (FOX) fueron solventadas con el sistema SACI. (Recomendación cumplida).	**RNC** El sistema SACI no cuenta con un mecanismo para bloquear a los usuarios de modo que inhabilite las cuentas de usuario después de 3 o más intentos

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	la medida implementada pierde eficacia. Vencimiento de palabras de paso e históricos de claves utilizadas Condición: No se cuenta con ningún mecanismo de vencimiento periódico de palabras de paso y el sistema no tiene previsiones para manejar históricos de palabras de paso.			fallidos de usuario y clave. **RNC** No se ha implementado aún un mecanismo que permita controlar la expiración de contraseñas o claves de acceso; tampoco se ha implementado un manejo de histórico de claves.
	Desactivación de usuarios Condición: El sistema de recaudación no cuenta con una opción de desactivado por lo que al momento de que un funcionario deje de laborar para la Institución no es factible bloquear el acceso con el usuario que se había creado para esa persona.	2. Estructurar un proceso de paralelo ordenado que permita consolidar una transición ordenada del sistema actual al nuevo sistema.	2. Esa transacción se llevó a cabo en el primer trimestre del 2004 y la misma fue exitosa. (Recomendación cumplida).	**RNC** El sistema no permite desactivar usuarios, sin embargo cabe recalcar que actualmente para bloquear el acceso a algún usuario se procede a quitarle los privilegios en la aplicación.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Ambiente instalado en las estaciones de trabajo Condición: Actualmente el SACI está instalado en todos los centros de recaudación con excepción de Procomer y se está utilizando para la impresión oficial de las facturas (recibos de dinero). Es importante señalar que el servidor de base de datos está instalado en modo local con las opciones del Enterprise Manager del SQL Server habilitadas de manera que un usuario utilizando esta herramienta puede acceder y modificar cualquier registro de la base de datos sin dejar ningún rastro.	3. Eliminar la impresión de facturas desde el SACI y mantener su impresión desde el sistema de recaudación hasta tanto no se hayan corregido y subsanado todas las debilidades que presenta el SACI.	3. Las fallas mencionadas fueron corregidas, por lo cual el sistema ha venido realizado el proceso de facturación de manera correcta. (Recomendación cumplida).	**RPC** Se han realizado las gestiones necesarias de modo que en las estaciones de los usuarios no se tenga instalado este tipo de software, sin embargo actualmente se cuenta con 2 estaciones las cuales aún tienen incorporado el Enterprise Manager.
	Registro de notas de crédito Condición: El sistema permite que se emita una nota de crédito asociada a una factura cuyo monto es superior a la factura previamente emitida. De igual forma es posible registrar una nota de crédito cuya fecha de registro es anterior a la factura a la cual se está asociando.	4. Incorporar validaciones en los procesos de registro de notas de crédito para evitar que se puedan generar notas de crédito con montos superiores a las facturas previamente definidas.	4. El módulo de notas técnicas nunca fue utilizado en el sistema, por ende la parte de ingresos pedirá que el mismo sea eliminado. (Recomendación no cumplida que ha perdido vigencia).	**RNV** Actualmente no se están usando notas de crédito en el sistema, denegando la posibilidad de incorporar una nota de crédito superior al monto de una factura, ni ingresarla con una fecha previa a la fecha de la factura.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Modificación de la fecha de emisión de una factura. Condición: El sistema permite al usuario escoger dentro de un calendario la fecha que aparecerá impresa y se almacenará como fecha de emisión del recibo de dinero (factura). Así es posible registrar fechas del 2000 o del 2004 y en todos los casos el sistema las acepta, con lo que se evidencia que no existe ninguna validación de razonabilidad de la fecha especificada por el usuario. Por otra parte, a pesar de que en el recibo se imprime la fecha seleccionada por el usuario, a nivel de la base de datos se almacena la fecha de registro y el detalle de la factura (rubros) se graba la fecha que se imprimió en la factura.	5. Revisar los procesos de inserción de información en la base de datos para los procesos de facturación para asegurar que se grabe la misma fecha tanto a nivel del encabezado de la factura como del detalle de ésta. Revisar además que se grabe el tipo de cambio en forma correcta en el detalle de las facturas.	5. La recomendación elaborada en este punto fue subsanada con la creación del sistema de ingresos (SACI), por lo cual en este momento no presenta este problema. (Recomendación cumplida).	**RNC** Actualmente no se ha modificado la interfaz de usuario de modo que inhabilite la posibilidad de que los usuarios puedan elegir la fecha de emisión.
	Captura del tipo de cambio a utilizar en la facturación Condición: El sistema permite utilizar un tipo de cambio que no corresponde a la fecha en la que se está emitiendo la factura.	6. Eliminar las opciones que posee el sistema para seleccionar la fecha de emisión de la factura y la fecha de referencia del tipo de cambio.	6. Las fechas de la factura y el tipo de cambio, el sistema SACI las asigna automáticamente al momento de elaborar la factura y ningún usuario puede variar esa información. (Recomendación cumplida).	**RNC** Es factible aún utilizar un tipo de cambio no correspondiente a la fecha en la que se está emitiendo la factura.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Almacenamiento del tipo de cambio utilizado en la base de datos Condición: En los rubros cuya tarifa es en dólares y que son cobrados en las facturas se registra un valor de tipo de cambio incorrecto en vista de que almacena el tipo de cambio dividido por 100.	7. Incorporar bitácoras de todas las anulaciones que se realicen de manera que se pueda identificar el usuario que las realizó y la fecha en que se efectuaron.	7. Este punto no se realiza debido a que nunca se contempló desde su creación del sistema la incorporación de bitácoras. (Recomendación no cumplida que mantiene vigencia).	**RNC** No se han realizado aún las modificaciones del caso para subsanar dicho hallazgo.
	Utilización de tipos de cambio diferentes para un mismo rubro. Condición: En vista de que el sistema permite seleccionar varias veces durante el proceso de facturación la fecha de referencia del tipo de cambio a utilizar es posible facturar un mismo rubro utilizando dos tipos de cambio diferentes.			**RNC** Se pudo determinar mediante las pruebas realizadas que el sistema aún permite el ingreso de tipos de cambio diferentes para un mismo rubro.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Relacionar facturas con depósitos Condición: El proceso de relacionar facturas con depósitos presenta problemas de tipo operativo ya que no es factible definir un nuevo depósito bancario y relacionar facturas a éste desde la pantalla que ofrece el sistema. Se encontró que existe un método alterno que está disponible en el reporte de cierre de caja a través del cual se relacionan una factura con un depósito y luego de esto es factible devolverse al proceso de vinculación de facturas a depósitos y relacionar otras facturas. Sin embargo, en estos casos el sistema presenta el problema de que no actualiza en forma correcta el monto total del depósito y luego se producen inconsistencias en la generación de reportes.	8. Revisar el proceso que permite relacionar facturas con depósitos para que sea factible incluir un nuevo depósito y luego asociarle facturas. Verificar que el proceso de acumulación a nivel del depósito corresponda con la sumatoria de facturas registradas.	8. La recomendación elaborada en este punto fue subsanada con la creación del sistema de ingresos (SACI), por lo cual en este momento no presenta este problema. (Recomendación cumplida).	**RC** No se constató la existencia de errores en el proceso de relacionar facturas con depósitos.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Validaciones a nivel de catálogos Condición: A nivel de catálogos de departamentos, bancos y estaciones el sistema no controla que no existan duplicados a nivel de descripción. Con respecto al catálogo de cuentas corrientes verifica que no se pueda registrar un número de cuenta ya existente pero no hace la validación considerando el banco en el cual se tiene la cuenta corriente de manera que no es factible registrar dos cuentas corrientes con la misma numeración pero pertenecientes a dos bancos diferentes. Esto es un problema menor a nivel de la operativa del sistema pero a nivel de programación evidencia un error de tipo conceptual con respecto a la forma en que debe realizarse la validación.	9. Incorporar validaciones en los mantenimientos de los catálogos para que no se puedan registrar descripciones duplicadas.	9. Los catálogos no permiten que sea ingresada información que actualmente se encuentre almacenado, es decir datos duplicados. (Recomendación cumplida).	**RNC** No se está validando aún a nivel de catálogos la existencia de duplicados en la descripción.
	Operación actual del sistema. Condición: El SACI se encuentra instalado en la mayoría de las cajas recaudadoras con excepción de Procomer y Limón donde se han tenido problemas para instalar la aplicación. En todos los lugares donde se tiene instalado el sistema se			**RC** Cabe mencionar que actualmente se tiene instalado el sistema en Procomer y en Limón. Por otra parte se cuenta con un modulo de exportación de datos para la actualización de la Base de Datos.

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	está usando para realizar la facturación oficial de los servicios. No se utiliza para registrar la información de depósitos ni tampoco para preparar los envíos que se realizan al MAG. Tampoco es usado para remitir los datos que se consolidan en oficinas centrales. Todo este conjunto de operaciones se están llevando a cabo en el sistema desarrollado en Fox y conocido como Recauda. En el sistema desarrollado en FOX se están registrando los ingresos percibidos luego de haber emitido la factura oficial con el SACI. Este tipo de manejo de los sistemas tiene el inconveniente de que se está aplicando un proceso de redigitación que no se está conciliando. Inclusive en pruebas realizadas que escapan el alcance de la auditoría al sistema se pudo evidenciar que existe una gran cantidad de diferencias entre los montos que reportan ambos sistemas como ingresos desde el mes de setiembre 2003. Por otra parte, es conveniente indicar que en las indagaciones realizadas se nos informó que el sistema SACI a pesar de haber sido aceptado formalmente todavía está en fase de			

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	pruebas y que hay procesos que no han sido probados. Esto provoca mayores dificultades porque se está usando un sistema incompleto y que tiene problemas operativos para emitir facturas oficiales y posteriormente se vuelven a registrar los datos de ingresos en el sistema oficial sin efectuar cuadres básicos que evidencien la consistencia de los datos.			
	Registro de formularios Condición: El sistema maneja en forma incorrecta los rangos de los formularios que se registran para ser entregados a los centros de recaudación. De esta forma se pudo evidenciar que el sistema pierde formularios previamente registrados ya que posee controles insuficientes sobre los rangos que son digitados.	10. Revisar los procesos de registro de formularios para evitar que se pierdan formularios por problemas en la especificación de los rangos.	10. Actualmente este proceso funciona correctamente, por lo que puede ser verificado mediante la emisión de los reportes. (Recomendación cumplida).	**RC** Se pudo constatar que el sistema cuenta con validaciones para un adecuado registro de formularios según pruebas efectuadas.
	Caída del sistema por agotamiento de formularios asignados Condición: Se determinó que el sistema presenta un problema de programación que provoca que la aplicación se caiga cuando el usuario se encuentra utilizando el proceso de facturación y se agotan los formularios	11. Revisar la lógica del sistema para corregir el problema de programación que provoca una caída de la aplicación cuando se agotan los formularios asignados a una caja de recaudación.	11. La recomendación elaborada en este punto fue subsanada con la creación con el sistema de ingresos (SACI), por lo cual en este momento no presenta este problema. (Recomendación cumplida).	**RC** En las pruebas realizadas no se presentaron caídas del sistema por agotamiento de formularios.

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	que se tienen disponibles en un centro de recaudación.			
	Pago de un recibo utilizando dinero en efectivo y un depósito bancario Condición: El sistema permite que se pueda registrar un recibo de dinero que será cancelado utilizando dinero en efectivo y un depósito bancario. La transacción es aceptada pero al momento de tratar de vincular el recibo con los depósitos bancarios este no está visible con lo que el monto en efectivo previamente recibido no puede ser registrado en ningún depósito ni aparece visible para efectos del cierre de la caja.	12. Revisar la lógica del sistema para evitar que se pierdan recibos de dinero compuestos por dinero en efectivo y depósitos bancarios y que sea factible registrar el depósito del dinero en efectivo recibido.	12. El sistema solamente recibe depósitos al momento de cancelar el monto de una factura. (Recomendación no cumplida que ha perdido vigencia).	**RNV** Actualmente no se están ingresando en el SFE el registro de dinero y depósitos para el pago de un recibo.
	Registro de facturas pagadas con depósito bancarios. Condición: Se determinó que el sistema permite el registro de pagos de servicios con depósitos bancarios previamente registrados; sin embargo, al momento de realizar el reporte del cierre de cajas, este tipo de ingresos no aparecen desglosados en la impresión correspondiente. Igual situación se presenta con el caso de notas de crédito emitidas o recibidas como forma de pago.			**RC** Actualmente no se está utilizando el reporte de cierre de caja, solo el cierre de caja mensual, el cual no presenta errores de programación.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Anulación de facturas vinculadas con notas de crédito. Condición: El sistema permitió emitir una orden de crédito para una factura y posteriormente fue factible anular esa factura.	13. Incorporar validaciones para que no se permita la anulación de una factura que fue previamente vinculada con la emisión de una nota de crédito. De igual forma, eliminar las opciones de reactivación de una factura anulada.	13. Actualmente no se está utilizando las notas de crédito, por ende el área financiera debe analizar la posibilidad de eliminar esta opción para todos e informar a la Sección de Informática de la decisión final para realizar el cambio respectivo. Actualmente se encuentra a la espera de dicha resolución. (Recomendación no cumplida que mantiene vigencia).	**RNV** Actualmente no se están registrando la anulación de facturas
	Facturación de certificados. Condición: El sistema permite registrar la facturación de un certificado y la entrega de más de un formulario de certificado. En estos casos se cobra solo el monto de un certificado y se registra la entrega	14. Revisar la lógica de programación del proceso que controla el manejo de certificados en la emisión de facturas para que exista consistencia entre la cantidad de formularios facturados y los que se registran como entregados. De la misma forma, verificar que no se puedan registrar certificados duplicados.	14. La recomendación elaborada en este punto fue subsanada con la creación con el sistema de ingresos (SACI), por lo cual en este momento no presenta este problema. (Recomendación cumplida).	**RC** Actualmente existen controles para determinar si un certificado no ha sido cobrado.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Control de entrega de formularios Condición: El sistema permite registrar en forma duplicada la entrega de un mismo certificado.			**RC** Se cuenta actualmente con un mecanismo de validación para evitar la entrega duplicada de formularios.
	Asignación de recibos a un depósito Condición: El sistema permite asociar más de un recibo a un depósito pero al momento de realizarlo no actualiza el monto total del depósito. Esto provoca una serie de inconsistencias en los reportes que luego produce el sistema.			**RC** Actualmente no se está registrando más de un recibo a un depósito.
	Asociación de formularios con tarifas donde aplican. Condición: El sistema permite identificar los rubros en los cuales se debe entregar certificados u otro tipo de formularios al cliente. De esta manera al momento de facturación se activan opciones para tratar de controlar la entrega de los citados formularios. Si bien es cierto el sistema permite realizar la vinculación correspondiente, la forma de implementación es muy rígida ya que no se permite hacer modificaciones o borrados de relaciones previamente registradas.	15. Revisar la programación del proceso de definición de tipos de formularios para que se realice de una manera más amigable la asociación de formularios con las tarifas donde estos aplican y sea factible en caso necesario eliminar alguna asociación previamente realizada luego de realizadas las verificaciones de integridad referencial requeridas.	15. Este proceso es realizado satisfactoriamente por el sistema. (Recomendación cumplida).	**RNC** No se ha implementado la posibilidad de poder modificar o borrar las relaciones registradas.

SISTEMA	DESCRIPCIÓN BREVE	RECOMENDACIÓN	COMENTARIOS DE LA ADMINISTRACIÓN	ESTADO
	Modificación de descripciones en los catálogos. Condición: El sistema permite modificar descripciones de departamentos, lugares de captación, y bancos a pesar de existir información vinculada a las descripciones modificadas.	16. Incorporar lógica en los sistemas que impida que se modifiquen descripciones en los catálogos si existen registros que hacen referencia a esas descripciones.	16. La recomendación elaborada en este punto fue subsanada con la creación del sistema de ingresos (SACI), por lo cual en este momento no presenta este problema. (Recomendación cumplida).	**RNC** No se ha implementado un mecanismo de validación para evitar la modificación en descripciones, cuando ya existen transacciones asociadas.
	Preparación de envíos Condición: El proceso habilitado para generar los envíos no despliega en pantalla ninguno de los depósitos que están pendientes de envío y por lo tanto no es factible completarlo.	17. Revisar los procesos de envío, cierre mensual y exportación e importación de datos que presentan problemas de funcionamiento. Incorporar al proceso de importación/exportación cifras de control de la información que debe ser cargada en la base de datos consolidada.	17. El proceso de importación / exportación presenta el inconveniente, el cual corresponde a que si un número de depósito específico se repite, la información no viaja a la base de datos central, se cuenta con un sistema para cambiar el número de depósito en la estación donde se elaboró la factura, pero cuando se vuelve a realizar la importación no viaja la asociación entre la factura y el nuevo depósito. Los procesos de envió y cierre mensual si funciona de forma correcta. Con la creación de la nueva aplicación vía web se estará solucionando esta recomendación. (Recomendación no cumplida que mantiene vigencia).	**RC** Se cuenta actualmente con una pantalla para verificar los depósitos pendientes de envío.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Cierre mensual. Condición: Este proceso depende de la ejecución correcta de los envíos y como estos no están operando, tampoco esta opción funciona correctamente.			**RC** No se constato la existencia de errores en el proceso de cierre mensual.
	Importación y exportación de datos Condición: La opción que tiene el sistema para importar y exportar datos para lograr el proceso de consolidación de información no está operando de manera correcta y carece de cifras de control. Además no se tienen controles que limiten la posibilidad de cargar dos veces un mismo archivo.			**RC** Actualmente se realizan procesos de importación y exportación sin inconvenientes, en donde se limita la posibilidad de cargar un mismo archivo dos o más veces.
	Reportes de ingresos por bancos y depósitos o cuentas. Condición: Su contenido es incorrecto ya que no incluye los depósitos recibidos por el cajero como pago a facturas emitidas en la fecha en proceso. Por otra parte el monto de los depósitos realizados por el cajero no es consistente con el monto efectivamente registrado como depositado.	18. Revisar los reportes de ingresos por bancos, facturas nulas, consecutivos por lugar de recaudación, saldos de facturación por lugar de captación y saldos de documentos que presentan problemas de tipo operativo.	18. Los reportes mencionados en este punto funcionan de manera correcta. (Recomendación cumplida).	**RC** Actualmente este reporte muestra los depósitos recibidos por el cajero como pago a facturas emitidas en la fecha en proceso de manera satisfactoria.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Reporte de facturas nulas Condición: El reporte de facturas nula omite la fecha en que la factura fue anulada y el usuario que la anuló, datos que son relevantes para el control interno de la operación.			**RNC** Este reporte no muestra aún la fecha en que la factura fue anulada, la fecha que se despliega en el informe es la fecha de emisión de la factura, por lo tanto dicho hallazgo se encuentra pendiente.
	Reporte de consecutivos por lugar de recaudación. Condición: El título del reporte no coincide con el contenido. El contenido pareciera que es de facturas emitidas por lugar de captación y no guarda relación con lo que se indica en el menú del sistema.			**RC** Actualmente no se presentan diferencias entre el titulo del reporte y el contenido, por lo tanto se pudo verificar la corrección al hallazgo.
	Reportes de saldos de facturación por lugar de captación y de saldos de documentos. Condición: Ambos reportes producen un error de ejecución y la aplicación tiene una caída abrupta.			**RC** No se pudo localizar la existencia de este reporte dentro del menú del sistema, por otra parte ninguno de los reportes desplegados en esta visita se presentó errores de ejecución o repercutieron en caídas del sistema.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Impresión de la factura (recibo de dinero). Condición: El reporte de la factura contiene datos relevantes como el número de factura, el usuario que lo está imprimiendo, la fecha de la factura, el tipo de cambio y fecha del tipo de cambio, la caja donde se está imprimiendo, el detalle de los servicios facturados y el total de la factura. Sin embargo omite la impresión de otros elementos importantes tales como: forma de pago utilizada (efectivo, nota de crédito o depósito) y los datos de identificación del depósito o nota de crédito utilizados como forma de pago.	19. Mejorar la impresión del detalle de la factura para que se indique cuánto fue el monto cancelado en efectivo, con depósitos y notas de crédito y se muestre el detalle de los números de depósito, banco y cuenta corriente que forman parte del pago, al igual que los números de notas de crédito utilizadas para la cancelación de la factura.	19. La impresión de la factura actualmente no hace mención ni a notas de crédito, ni efectivo porque no se utilizan esos tipos de pago. (Recomendación cumplida).	**RNC** A la fecha no se han hecho las modificaciones requeridas al informe de impresión de la factura de modo que muestre información detallada referente a la forma de pago.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
Reporte de cierre de caja	Condición: Este reporte presenta algunos problemas derivados de errores de procesamiento. En primera instancia los totales que da para una caja recaudadora no corresponden con el total recaudado por dicha caja. Además como reporte de cierre de caja está mal conceptualizado ya que el reporte lo que está mostrando son de los depósitos que el cajero hizo durante el día y además el dato del monto total de cada depósito es incorrecto. Un reporte de cierre de caja debiera indicar con todo el detalle posible cuáles facturas se emitieron, en cuales de ellas el pago fue hecho en efectivo, en cuáles con depósito, en cuales con notas de crédito. Además debe indicar cuáles facturas anuló y qué depósitos bancarios hizo durante el día. A partir de ahí se puede entonces elaborar el cierre de caja desde el punto de vista de dinero en efectivo que debe tener el cajero.	20. Replantear el reporte de cierre de caja para que presente un detalle ordenado de todas las facturas emitidas durante el día con su correspondiente monto en efectivo, monto en depósitos, monto en notas de crédito. De igual forma que presente un detalle de los depósitos bancarios recibidos durante el día, las notas de crédito recibidas durante el día, las facturas anuladas durante el día, las notas de crédito anuladas y un resumen de los depósitos realizados por el cajero de dinero en efectivo recibido, de manera que en un solo reporte se tenga toda la operativa del cajero resumida para cada día.	20. Actualmente el proceso de cierre de caja no se realiza, debido a que el departamento financiero no lo trabaja de esta forma. (Recomendación no cumplida que ha perdido vigencia).	**RNV** No se está utilizando este reporte actualmente, por lo tanto no es necesario hacer las correcciones a dicho informe, sin embargo es deseable omitir esta opción del menú que despliega el sistema.

SISTEMA	*DESCRIPCIÓN BREVE*	*RECOMENDACIÓN*	*COMENTARIOS DE LA ADMINISTRACIÓN*	*ESTADO*
	Reporte de facturas sin depósito. Condición: En este reporte se omite aquellas facturas que se pagaron una parte en efectivo y otra con depósito. Esto es una debilidad que posee el sistema que produce que esa factura para efectos de su liquidación no aparezca por ningún lado con el consiguiente riesgo en cuanto al destino que tome el dinero efectivo que se recibió.	21. Considerar el desarrollo de módulos para facilitar la conciliación bancaria de las cuentas de depósito utilizadas y para el control de ingresos del fideicomiso, así como para habilitar medios de consulta para el área de contabilidad del MAG y para lograr integración con el sistema de presupuesto para lograr consolidar una aplicación que brinde servicios de forma integral.	21. Todavía se encuentran en análisis por parte del área financiera el desarrollo de un sistema que brinde servicios de manera integral. La Sección de Informática esta a la espera de la decisión final sobre esta recomendación. Con la creación de la nueva aplicación se tomará en cuenta la decisión de dicha área. (Recomendación no cumplida que ha perdido vigencia).	**RNV** No es necesario para efectos operativos realizar las correcciones del caso, actualmente en el SFE solo están llegando facturas con depósito.

4.2 RECOMENDACIÓN

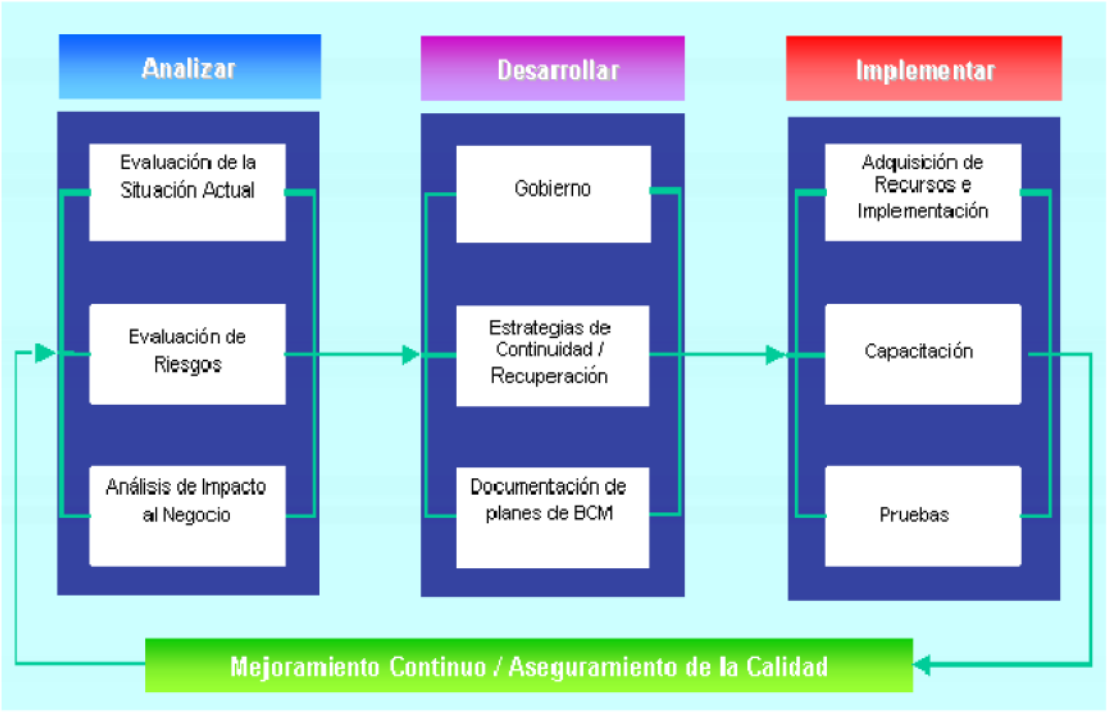
4.2.1 Remitir el cronograma de actividades (detalle de las actividades vinculadas con el nombre de los responsables y fechas de ejecución) relacionado con la atención de las recomendaciones que se encuentran en estado de RPC y RNC.

ANEXO 1

ANEXO 1

ADMINISTRACIÓN DE LA CONTINUIDAD DE NEGOCIO

METODOLOGÍA DE BCP



RECOMENDACIÓN DE IMPLEMENTACIÓN A CONSIDERAR POR LA ENTIDAD

Generar un diagnóstico del estado de madurez de las definiciones de continuidad, relacionadas con:

- Requerimientos regulatorios del sector, el gobierno, etc.
- Actividades actuales de continuidad en las funciones de servicio.
- Tipo de planes de atención de emergencia y salvaguarda del personal.
- Planes de recuperación de desastres para la plataforma tecnológica.

Acotar el alcance de la implementación del BCP

- Definir qué objetivos estratégicos de su actividad desea cubrir en forma prioritaria en una primera fase.
- Identificar los procesos o áreas de servicio asociados a esos objetivos.
- Establecer el proyecto de implementación del BCP.

Defina la implementación del plan considerando:

- El *sponsor* del proyecto general
- Desarrollo del plan del proyecto y su presupuesto
- La estructura y la administración del proyecto
- Los roles y responsabilidades de los involucrados en el plan

ESTRATEGIA DE IMPLEMENTACIÓN

Realizar un trabajo continuo de la implementación del modelo.

- Establecer monitoreo continuo sobre el cumplimiento de las actividades administrativas definidas en el plan.
- Establecer indicadores de gestión para medir el cumplimiento.
- Evaluar periódicamente el nivel de madurez de implementación.

Factores clave de éxito

- Gestionar el apoyo y liderazgo de la alta gerencia
- Definir un líder de proyecto, idealmente un líder de procesos
- Identificar el personal idóneo que debe participar en cada fase
- Realizar actividades de sensibilización.
- Realizar actividades de transferencia de conocimiento al personal.
- Utilizar enfoque de procesos y no de tecnología

BENEFICIOS

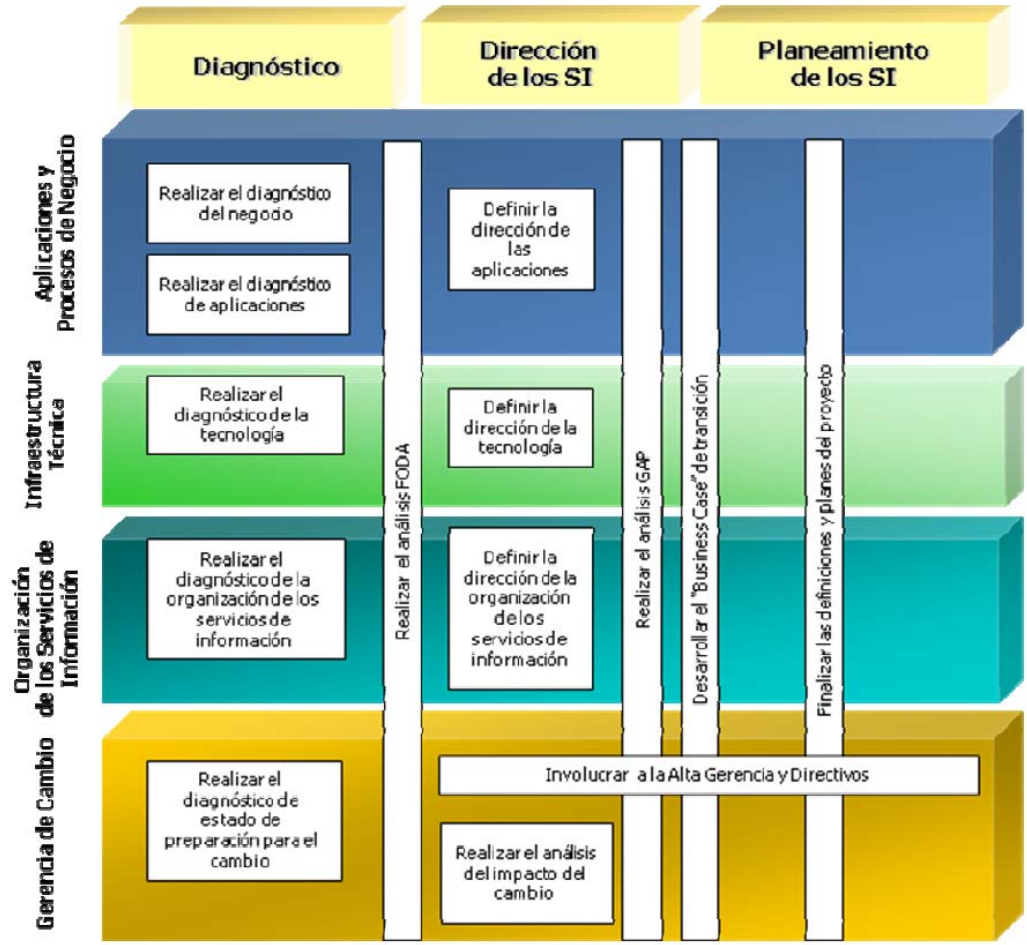
- Gestión de la supervivencia de las operaciones críticas de la Institución ante un escenario de Desastre.
- Ventajas competitivas en el sector social.
- Fortalecimiento de la imagen institucional, generando confianza en sus usuarios, beneficiarios, y público en general.
- Cubrimiento de aspectos normativos o contractuales con el sector, el estado y los Miembros de la Junta Directiva.

ANEXO 2

ANEXO 2

PLANEACION ESTRATEGICA DE TECNOLOGIA

METODOLOGÍA PARA DISEÑAR UN PLAN ESTRATÉGICO DE TI



* * * * *

ANEXO 3

EVALUACIÓN DE LA CALIDAD FUNCIONAL DE LOS SISTEMAS DE INFORMACIÓN Y DE LA SECCIÓN DE INFORMATICA

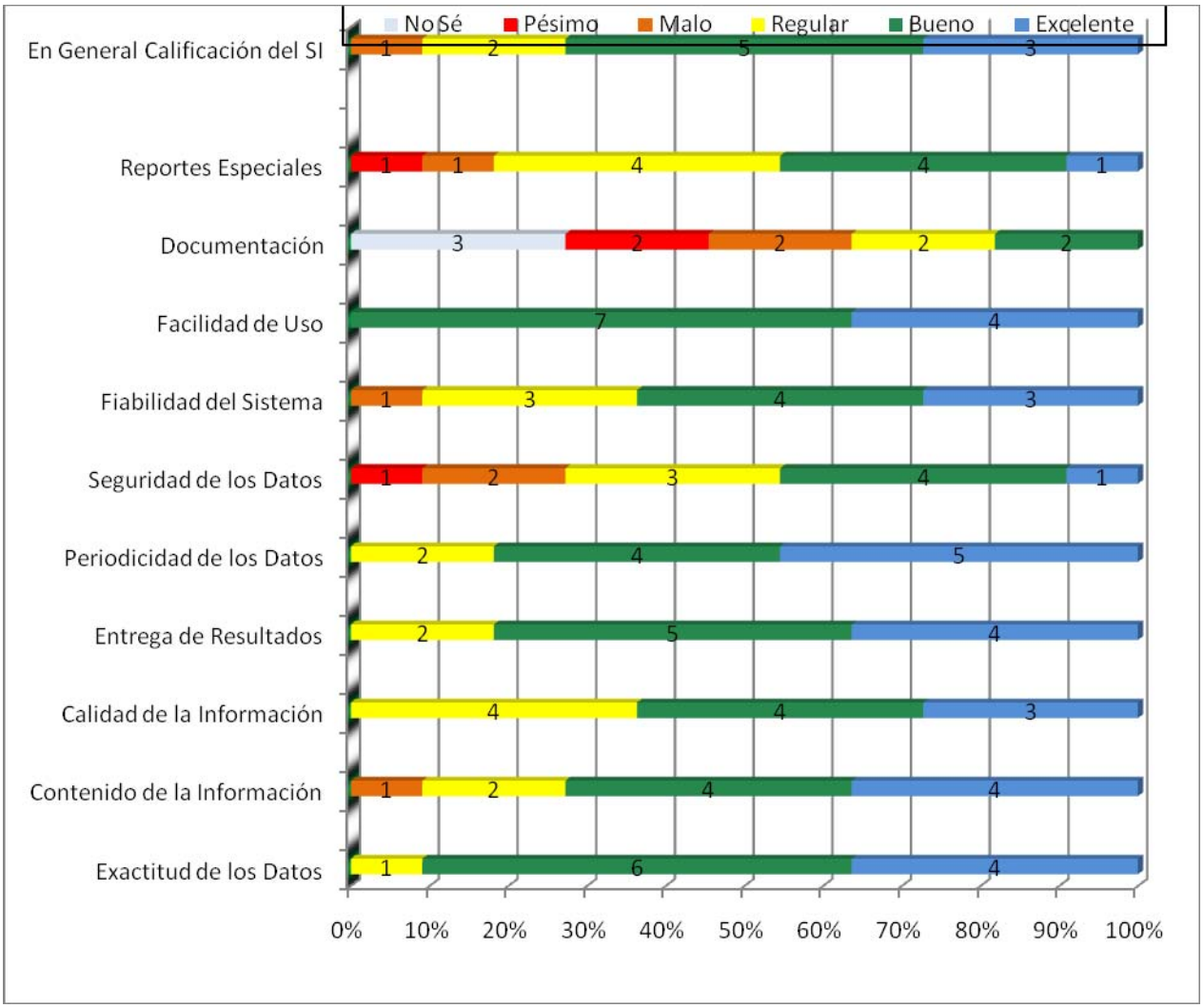
En este anexo se muestra el resultado de la evaluación realizada respecto a la calidad funcional de los sistemas de información del SFE, según la percepción de los usuarios finales.

Los sistemas evaluados fueron los siguientes:

SISTEMA	***USUARIO FINAL ENTREVISTADO***
Planillas	Claudio Fallas Cortes
Laboratorio	Sonia Mesén Juaréz
	Melissa Meléndez Méndez.
	Roger Ruiz Zapata
Cuarentena Agropecuaria	Warner Herrera Méndez
Presupuesto	Kathy Aguilar Chaverri
	Alexander Gómez Chacón
Constancia de Inspección y Autorización de Tránsito	Warner Herrera Méndez.
Exportaciones	Fanny Sanchez Oviedo
	Karen Fernández
Vigilancia Fitosanitaria	Gerardo Granados Araya
Administración y Control de Ingresos	Douglas Aguilar Pérez

EVALUACIÓN AL SISTEMA DE INFORMACIÓN IMPLANTADO EN EL SFE

El detalle de la evaluación de la calidad funcional del sistema que se encuentra actualmente en producción según los usuarios, se muestran en el gráfico siguiente:



PERCEPCIÓN DE LOS USUARIOS FINALES RESPECTO AL SERVICIO RECIBIDO POR LA SECCIÓN DE INFORMÁTICA

El detalle de la evaluación de la percepción de los usuarios finales respecto al servicio recibido por el área de informática se muestra en el gráfico siguiente: