INFORME DE AUDITORÍA INTERNA AI JPS N° 12-2017

ÁREA DE SISTEMAS

TEMA:

VERIFICACIÓN DE POLÍTICAS, PROCEDIMIENTOS Y ESTÁNDARES DEFINIDOS POR EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN RELACIONADO CON LA GESTIÓN DE LA BASE DE DATOS INSTITUCIONAL

PREPARADO POR:

LIC. ANDRÉS MARTÍNEZ PORRAS
PROFESIONAL II

LIC. WEN JIE ZHEN WU
PROFESIONAL II

JUNTA DE PROTECCION SOCIAL
Lilliana Rojas
06 SEP 2017

GERENCIA GENERAL

24 DE AGOSTO DE 2017

JUNTA DE PROTECCION SOCIAL
TECNOLOGIAS DE INFORMACION
06 SEP. 2017
2:13pm
RECIBIDO

DIRIGIDO A:

GERENCIA GENERAL

DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN

INDICE DEL INFORME

RESUMEN EJECUTIVO

Informe de Auditoría N° 12-2017
"Estudio sobre la verificación de políticas, procedimientos y estándares definidos por el Departamento de Tecnologías de la Información relacionado con la gestión de la base de datos institucional."

En cumplimiento al Plan Anual de Trabajo para el año 2017, se realizó un estudio sobre la verificación de políticas, procedimientos y estándares definidos por el Departamento de Tecnologías de la Información relacionado con la gestión de la base de datos institucional. Este estudio cubrió el período comprendido entre el 01 de julio 2015 al 31 de diciembre 2016, ampliando el mismo cuando fue considerado necesario.

El objetivo general del presente estudio es comprobar los controles que lleva el Departamento de Tecnologías de la Información sobre la base de datos institucional, tomando como base la normativa, las políticas, los procedimientos y los estándares referentes a la administración de base de datos.

Cabe destacar, que la Auditoría Interna en su función asesora y fiscalizadora realiza estudios en los cuales por medio de las recomendaciones giradas en sus *"Informes de Auditoría"*, trata de proporcionar una garantía razonable de que las actuaciones del jerarca, los titulares subordinados y todos los colaboradores de la Institución, se apeguen a sanas prácticas, y se ejecuten dentro del marco técnico y legal vigente, por lo que se emiten recomendaciones las cuales se dirigen a fortalecer la estructura de control interno implantada por las diferentes dependencias administrativas.

Del estudio efectuado por esta Auditoría Interna se determinaron las siguientes debilidades:

- ✓ En las políticas de administración de las tecnologías informáticas, definen la figura del encargado de seguridad, sin embargo, en la estructura organizacional de esa Unidad no existe, por tal razón, no se efectúa como parte de sus tareas, el informe mensual de accesos no permitidos o accesos inadecuados.

- ✓ No se cuenta con un programa que encripte información confidencial, en este caso, el nivel de riesgo va en forma proporcional al tipo de información que se almacene en los equipos de los usuarios.

- ✓ No se ha lanzado una campaña de concientización en materia de seguridad a los funcionarios de la Junta de Protección Social, lo cual es indispensable para que el personal conozca y tenga presente, las políticas referentes a la seguridad de la información.

- ✓ No se tiene una política para el manejo de datos históricos, la información histórica almacenada en una base de datos, consume gran cantidad de la capacidad de almacenamiento y el uso que se le da a los mismos puede ser mínimo y en algunos casos nulo, lo que eventualmente demandarían un mayor tiempo de acceso a los datos que realmente están en uso.

- ✓ No se están generando informes relacionados con la calidad de los servicios prestados por terceros al finalizar los contratos o al renovarlos, este monitoreo sería útil para conocer si la inversión en este tipo de contrataciones está dando el resultado esperado, igualmente si es procedente la continuación de los servicios.

- ✓ El Departamento de Tecnologías de la Información, no es uniforme al aplicar el modelo de estándar de desarrollo y creación de base de datos, en lo que respecta a: *creación de columnas o campos (y sus nombres)*, *creación de procedimientos almacenados* y *en la creación de trigger*. El propósito de la asignación de estándares, es dar un enfoque consistente y un lenguaje común en entornos con múltiples equipos de desarrollo.

- ✓ Finalmente, se observó que cuando un desarrollador de sistemas se encuentra laborando en un servidor de desarrollo y tiene abierto simultáneamente un servidor de producción, al darse esta situación, la información de ambos servidores interactúa, lo que puede ocasionar, eventualmente, que la información contenida en la base de datos sea alterada por error.

Cabe destacar que la Auditoría Interna en su función asesora y fiscalizadora realiza estudios en los cuales por medio de las recomendaciones giradas en sus *"Informes de Auditoría"*, trata de proporcionar una garantía razonable de que las actuaciones del jerarca, los titulares subordinados y todos los colaboradores de la Institución, se apeguen a sanas prácticas y se ejecuten dentro del marco técnico y legal vigente, por lo que las recomendaciones se dirigen a fortalecer la estructura del control interno implantada por las diferentes dependencias administrativas.

Por su parte, a la Administración, le corresponde valorar dentro de los plazos establecidos las recomendaciones emitidas por la Auditoría Interna, su implementación conllevaría la actualización de sus procedimientos o bien proponer medidas alternativas que reduzcan o eliminen las situaciones de riesgo determinadas sobre las operaciones que se llevan a cabo en forma diaria en la Institución, con las posibles implicaciones que ellas pueden originar sobre el patrimonio y los recursos públicos que administra la Junta de Protección Social y el efecto que dichas situaciones podrían tener sobre los acreedores de rentas.

1. INTRODUCCION.

1.1. Antecedentes del estudio.

El presente estudio se elaboró en cumplimiento del Plan Anual de Trabajo del Área de Sistemas para el período 2017.

1.2. Objetivo general del estudio.

Determinar los controles que lleva el Departamento de Tecnologías de la Información sobre la base de datos institucional, tomando como base las políticas, los procedimientos y los estándares referentes a la administración de base de datos.

1.3. Objetivos específicos

- Comprobar el cumplimiento de los controles y políticas relacionados con la base de datos institucional.

- Verificar el cumplimiento de las políticas y estándares definidos para la creación y modificación de los objetos de la Base de Datos institucional.

1.4. Alcance del estudio.

El estudio se basó en la comprobación del cumplimiento de políticas y estándares aplicados a la administración de la base de datos institucional, tomándose como parámetro el documento denominado *Manual Políticas de Administración Tecnologías de Información de Junta Protección Social*, así como los estándares definidos para la creación de objetos en la base de datos.

1.5. Período revisado.

Para la revisión de las políticas y estándares, se consideró el periodo comprendido de julio 2015 a diciembre 2016.

1.6. Metodología.

Para la realización de este estudio se consultó:

a) Ley General de Control Interno N° 8292 del 18 de julio del 2002, en cuanto a los artículos N° 8, N° 10, N° 15 y N° 16, referidos al Sistema de Control Interno.

b) Normas de Control Interno para el Sector Público, (Publicado en La Gaceta N° 26 del 6 de febrero del 2009), Normas N° 1.4, N° 1.5 N° 4.3, N° 4.4, N° 5.4, N° 5.5 y N° 5.6 sobre Responsabilidad de los Jerarcas y Titulares Subordinados respecto al Sistema de Control Interno, Protección y conservación del patrimonio, Exigencia de confiabilidad y oportunidad de la información, Gestión documental, Archivo Institucional y Calidad de la información.

c) Nota TI 77-14 3 febrero 2014

d) Normas Técnicas para la gestión y Control de las tecnologías de información

e) Manual de procedimientos del Departamento de Tecnologías de la Información

f) Manual Políticas de Administración del Departamento de Tecnologías de la Información

g) Estudio de Análisis de Capacidad de Servidores realizado por el Departamento de Tecnologías de la Información

h) Código fuente de los aplicativos del sistema

1.7. Procedimientos utilizados para efectuar el estudio.

- Recopilación de la normativa relacionada con el tema en estudio.
- Revisión de las políticas, procedimientos y estándares, relacionados con la base de datos institucional.
- Revisión de la Valoración del Riesgo efectuada por la Administración Activa, sobre la seguridad que rodea el acceso a la base de datos a través de los sistemas informáticos institucionales.

- Revisión de objetos de la base de datos conocidos como "trigger", de los procedimientos almacenados y de los estándares establecidos para la creación de columnas o campos en la base de datos.

- Revisión del sistema de seguridad de la consola de aplicaciones.

- Entrevistas a funcionarios del Departamento de Tecnologías de la Información que tienen a cargo el manejo y custodia de la base de datos.

- Recolección de documentos relacionados con la comunicación hacia los funcionarios, sobre la seguridad que deben observar en el uso de los sistemas de información computadorizados disponibles en la institución.

1.8. Normativa sobre deberes en el trámite de informes de Auditoría.

De conformidad con lo que establece la Contraloría General de la República, se transcriben los artículos N° 36, N° 37, N° 38 y N° 39 de la Ley General de Control Interno N° 8292, publicada en la Gaceta N° 169 de 4 de setiembre del 2002:

> ***"Artículo 36.- Informes dirigidos a los titulares subordinados***
>
> *Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*

c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.

Artículo 37.- Informes dirigidos al jerarca

Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.

Artículo 38.- Planteamiento de conflictos ante la Contraloría General de la República

Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

Artículo 39.- Causales de responsabilidad administrativa

El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios..."

2. RESULTADOS DEL ESTUDIO.

2.1. Verificación del cumplimiento de políticas, procedimientos y estándares.

2.1.1. Error en la redacción en una política

Según revisión efectuada al "Manual Políticas de Administración Tecnologías de Información de Junta Protección Social", se determinó que la Política I, referente a la Seguridad de la Información, en el apartado 4.3.5 *Gestión de aplicaciones*, contiene un error en el texto, específicamente en la página N° 18, de donde se extrae:

...

> *"El ambiente de producción es utilizado exclusivamente por el personal autorizado de desarrollo de sistemas."*

Precisamente el ambiente de producción, al contrario de lo que dicta la política mencionada, es donde se llevan a cabo las operaciones normales del procesamiento de datos producto del movimiento transaccional realizado por los usuarios de los sistemas, en tanto que en el ambiente de desarrollo, es en donde los profesionales en informática efectúan sus desarrollos y modificaciones y así lo aclaran las *Normas técnicas para la gestión y control de las tecnologías de información emitido por la Contraloría General de la República*, en el glosario:

> ***"Ambiente de producción*** *Conjunto de componentes de hardware y software donde se efectúan los procesos normales de procesamiento de datos, con sistemas e información reales.*
>
> ***Ambiente de desarrollo*** *Conjunto de componentes de hardware y software donde se efectúan los procesos de construcción, mantenimiento (ajustes, cambios y correcciones) y pruebas de sistemas de información."*

Si bien es cierto, que el Departamento de Tecnologías de la Información, tiene el ambiente de pruebas y el de producción debidamente separados, es importante que la política este correctamente redactada, para evitar inducir a error a los funcionarios en el momento de llevar a cabo sus labores cotidianas.

2.1.2 Ausencia de un Encargado de Seguridad

El señor Jairo Cruz Sibaja, funcionario del Departamento de Tecnologías de la Información, encargado de la base de datos, en entrevista realizada el 28 de setiembre del 2016, indicó que dicha unidad administrativa, no cuenta con un funcionario Encargado de Seguridad.

La política I, referente a la Seguridad de la Información, en el apartado 4.3.1 *Gestión de identidad de accesos*, en la página 13 cita:

> "...
> *El Encargado de Seguridad del Departamento de Tecnologías de Información debe registrar y monitorear los accesos a los sistemas de JUNTA PROTECCIÓN SOCIAL, a fin de detectar el uso indebido de los accesos suministrados a los usuarios. Así mismo deberá entregar un reporte con los usuarios y accesos otorgados al personal de los departamentos de JUNTA PROTECCIÓN SOCIAL cada mes."*

Por lo tanto, al no haber un encargado de seguridad, no se están generando los informes mensuales correspondientes a la labor de monitoreo de los accesos lo cual puede traer como consecuencia la inobservancia de accesos no permitidos o usos indebidos de accesos previamente suministrados.

2.1.3. Encriptación de la información

Según entrevista al señor Jairo Cruz, ya citada, no se cuenta con un programa que encripte información confidencial.

La política I, referente a la Seguridad de la Información, en el apartado 4.3.7 *Gestión de activos de la información*, en la página 20 cita:

> *"Todo computador o equipo que contenga información confidencial, deberá contar con un programa de encriptación o cifrado de los datos para el almacenamiento de la información."*

En este caso, el nivel de riesgo para la institución va en forma proporcional al tipo de información que se almacene en los equipos de los usuarios, de igual forma, la importancia de la información definirá si requiere ser encriptada para minimizar el riesgo institucional.

2.1.4. Concientización a los funcionarios en materia de seguridad informática

A la fecha de este informe, no se ha lanzado una campaña de concientización en materia de seguridad a los funcionarios de la Junta de Protección Social.

La política I, referente a la Seguridad de la Información, se creó con el siguiente propósito:

> *"PROPÓSITO*
> *Determinar los lineamientos que definen y dan soporte al sistema de gestión de seguridad de la información de la Junta de Protección Social (JUNTA PROTECCIÓN SOCIAL), con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información."*

En vista de lo anterior, en el apartado 4.3.10 *Gestión de activos de comunicación*, en la página 21, se estipuló lo siguiente:

> *"El Departamento de Tecnologías de Información deberá capacitar a los funcionarios al menos una vez al año respecto a las políticas de seguridad de la información."*

Para capacitar a los funcionarios de la institución en materia de seguridad, el Departamento de Tecnologías de la Información, por medio del señor Steve Calvo Cruz[1], está realizando una campaña de concientización, la cual será difundida por medio del correo electrónico y boletines que se desplegarán al iniciar la sesión en los equipos, para lanzar la campaña se requiere de la autorización de la jefatura de dicho departamento, sin embargo, a la fecha, la campaña no ha sido iniciada.

Es indispensable que el personal de la Junta de Protección Social, conozca y tenga presente, las políticas referentes a la seguridad de la información, por cuanto es responsabilidad de todo el personal cumplir con los lineamientos establecidos en dicha política y de la misma forma cumplir con el propósito para la cual fue creada.

2.1.5. Política para el manejo de la información histórica

Según revisión del *Manual de Políticas de Administración Tecnologías de Información* y entrevista al señor Jairo Cruz del 28 de setiembre del 2016, se constató que el Departamento de Tecnologías de la Información, no tiene una política para el manejo de datos históricos. La práctica utilizada por dicha unidad, consiste en que un asesor externo, (en este caso Joaquín Casaw) lleva a cabo respaldos de base de datos y limpia los datos que no se necesitan.

---

[1] El señor Steve Calvo Cruz, es parte de la empresa SPC Internacional S.A. contratada por el Departamento de Tecnologías de la Información, mediante Contratación Directa 2015 CD000353-PROV 03.

Tener una política del manejo de datos históricos ordenaría la forma de cómo se debe manejar esa información, así mismo, los funcionarios o personal externo encargados de hacer dicha labor tendrán la metodología clara para proceder de forma correcta con el tipo de datos citado.

Los datos históricos almacenados en una base de datos, consumen gran cantidad de almacenamiento y el uso que se le da a los mismos puede ser mínimo y en algunos casos nulo, lo que eventualmente demandarían un mayor tiempo de acceso a los datos que realmente están en uso.

2.1.6. Evaluación de los contratos de servicios profesionales constituidos en el área de TI.

El Departamento de Tecnologías de la Información, no está generando informes relacionados con la calidad de los servicios prestados por terceros al finalizar los contratos o al renovarlos.

En la consultoría llevada a cabo por la empresa Deloitte & Touche S.A. mediante Licitación Abreviada N° 2011 LA-00024-PROV y la cual consistió en un *Alineamiento e implementación de la normativa emitida por la Contraloría General de la Republica de tecnologías de información*, en la página 715 y subsiguientes, emite una "Guía de Seguimiento a Contratos de Proveedores" la cual incluye indicadores de cumplimiento de los contratos, asimismo, en las páginas de la 712 a la 715, anexó formularios para llevar a cabo la revisión citada.

Sobre el mismo tema las Normas técnicas para la gestión y el control de las tecnologías de información, en la norma 4.6 Administración de servicios prestados por terceros inciso e.) cita:

> *"Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados"*

Las políticas fueron creadas como normas fundamentales que deben regir aspectos de seguridad, calidad del servicio, control y monitoreo de los temas relacionados con las tecnologías de la información aplicadas en la Junta de Protección Social, si éstas no se cumplen, se estaría ante falta de controles que minimicen el riesgo, desmejora en los procesos relacionados con los sistemas de información, así como en la implantación de aquellas medidas necesarias para garantizar la seguridad de la información y el mejoramiento en los procesos.

2.2. Comprobación de los estándares de nomenclatura aplicados a los objetos de la base de datos

2.2.1. Nomenclatura en el nombre de las tablas

Se determinó, que el Departamento de Tecnologías de la Información, no aplica el modelo de estándar de desarrollo y creación de base de datos, en lo que respecta a la nomenclatura en la creación del nombre de las tablas.

Para verificar el cumplimiento del estándar citado, se extrajo una muestra del 10% de las tablas de bases de datos creados en el periodo de estudio, dando como resultado que las siguientes tablas no cumplen con el estándar:

Cuadro N° 1

Base de datos	Nombre de la tabla	Fecha creación	Observaciones
Jps_real	PE_TrasladosCorte	02/06/2016	No inicia con la sigla M ni describe el tipo de tabla
	MDP_CatParamClaseVenta	17/05/2016	No describe el tipo de tabla
	MDP_CatParamNORETIRO	21/06/2016	No describe el tipo de tabla
Perdba	RH_TiposPagos	14/01/2016	No inicia con la sigla M ni describe el tipo de tabla
	RH_HorarioEventos	14/01/2016	No inicia con la sigla M ni describe el tipo de tabla
	MRH_TiposLevantamiento	21/09/2015	No describe el tipo de tabla
	MCT_DiasEmpleado	05/02/2016	No describe el tipo de tabla
Presupuesto_db	AF_Movimientos	10/06/2016	No inicia con la sigla M ni describe el tipo de tabla
	CXP_ParamFactUsuario	21/06/2016	No inicia con la sigla M ni describe el tipo de tabla
	AF_Categorias	02/05/2016	No inicia con la sigla M ni describe el tipo de tabla

El Departamento de Tecnologías de la Información, estableció el siguiente estándar de nomenclatura para la creación de tablas:

> *" f) Nombre de una tabla*
>
> *Se construirá de la siguiente manera:*
>
> *M+<siglas del sistema>_<nombre tabla>+<tipo tabla>*

Donde:
M*: significa módulo y se escribe en mayúscula.*

Siglas del sistema*: mínimo 2 letras y máximo de 6 letras, en mayúscula*

Nombre tabla*: nombre significativo de la tabla mínimo de 5 letras y máximo 20 letras, donde para cada primer letra de cada palabra que se utilice, se escribe en mayúscula y el resto de manera consecutiva.*

Tipo de tabla: *el cual se refiere al siguiente código de 3 letras en minúscula:*

- *Catálogo* ***CAT***
- *Parámetros* ***PAR***
- *Histórico* ***HIS***
- *Movimientos* ***MOV***
- *Temporal* ***TMP"***

En el cuadro N° 1, en la columna de "*Observaciones*" se detallan las inconsistencias que tuvieron los nombres de las tablas con respecto al estándar.

Los estándares para el desarrollo de los sistemas de información, contiene los procedimientos básicos que regulan a los analistas y programadores para desarrollar la documentación del sistema, del programa, del usuario, de las operaciones del computador y de otros procedimientos pertinentes al sistema de información computadorizado, en particular esto permitirá que la organización disponga de documentación completa, adecuada y actualizada para todos los sistemas que se desarrollen.

2.2.2. Estándar para la creación de columnas o campos.

Se revisaron los nombres de los campos o columnas de las tablas de base de datos creadas entre julio del 2015 a diciembre del 2016, determinándose que ninguno de ellos cumple con el estándar definido por el Departamento de Tecnologías de la Información, como se demuestra en el siguiente cuadro:

Cuadro N°2
Ejemplo de una tabla creada sin los estándares.

CREATE TABLE AF_Categorias		
CodigoCategoria	Int	NOT NULL,
Nombre	varchar(255)	NOT NULL,
Cuenta	varchar(20)	NOT NULL,
CuentaDepreciacion	varchar(20)	NULL,
SeDeprecia	char(1)	NOT NULL,
PorcentajeDepreciacion	decimal(18,2)	NOT NULL,
EsSoftware	char(1)	NOT NULL,
PermiteTraspasos	char(1)	NOT NULL,
UsuarioRegistra	varchar(20)	NOT NULL,
FechaRegistra	datetime	NOT NULL,
CuentaDeterioro	varchar(20)	NULL,
CuentaReevaluacion	varchar(20)	NULL,
CuentaMejora	varchar(20)	NULL,
TipoValorResidual	char(1)	NULL,
CuentaGasto	varchar(20)	NULL,
CategoriaDesecho	int	NULL,
CONSTRAINT pk_af_categorias PRIMARY KEY CLUSTERED (CodigoCategoria), CONSTRAINT ckc_permitetraspasos_af_categ CHECK (PermiteTraspasos in ('S','N')), CONSTRAINT ckc_sedeprecia_af_categ CHECK (SeDeprecia in ('S','N')), CONSTRAINT ckc_tipovalorresidual_af_categ CHECK (TipoValorResidual is null or (TipoValorResidual in ('P','M'))))		

El Departamento de Tecnologías de la Información, definió de la siguiente manera el estándar para la creación de columnas o campos de las tablas:

> ***"g) Nombres de campos en una tabla***
> ...
> *Todo campo debe ser definido según el tipo de dato que va a contener, por ejemplo un campo tipo fecha debe ser almacenado como tal y con un formato donde se tome en cuenta cuatro dígitos para almacenar el año.*

Cuando un campo contenga valores predefinidos o rangos de posibles valores, éstos deben ser incluidos como una regla de validación dentro de la definición del campo en la tabla, ejemplo valores si o no se almacena "s" o "n" únicamente.

Si los campos a definir no deben aceptar valores nulos, esto debe quedar definido de forma implícita en la definición del campo en la tabla.

El nombre de un campo en una tabla se construirá de la siguiente manera:
***Tipo de campo + "_" + descripción para el campo** en (máximo 15 caracteres)*
2 caracteres + 1 carácter + 15 caracteres máximo = 18 caracteres máximo
El tipo de campo se refiere al siguiente código de 2 letras:

IDENTIFICADOR DEL CAMPO	NOMBRE	IDENTIFICADOR DEL CAMPO	NOMBRE
CA	CANTIDAD	UN	NUMERO
CE	CEDULA	OB	OBSERVACIONES
CO	CODIGO	PO	PORCENTAJE
DE	DESCRIPCION	SE	SEÑAL (BIT)
FE	FECHA	TP	TIPO
ID	IDENTIFICADOR	ES	ESTADO
IM	IMAGEN	HO	HORA
IN	INDICADOR	NM	NEMOTECNICO
MO	MONTO	TX	TEXTO

***Ejemplo del nombre de un campo de forma correcta:** FE_Recepcion" (fecha de recepción).*

Obsérvese que en el Cuadro N° 2, los nombres de los campos no están siguiendo el formato señalado, utilizando el código de dos letras (tal como se indica en el cuadro anterior), ni el resto del formato donde se incluye la descripción del campo.

Los estándares en informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las tecnologías de información, sin esas guías, se puede crear un desorden en los nombres de columnas y campos, lo cual eventualmente, podría demandar a la institución tiempo y recursos económicos, para el entendimiento y ordenamiento de dicho procedimientos.

2.2.3. Creación de procedimientos almacenados.

Se determinó que existen procedimientos almacenados en la base de datos institucional, que no guardan el estándar definido por el Departamento de Tecnologías de la Información.

Para verificar lo anterior, se tomó una muestra de 10 procedimientos almacenados, creados en la base de datos de julio del 2015 a diciembre 2016, de los cuales ninguno cumple con dicho estándar:

- AF_RegistraMovimientoDetVarios
- AF_AprobarReevaluacion
- AF_TraerActivoSinMovimiento
- AF_TraerActivoConMovimiento
- RH_RegistrarFirmaAsistencia240516
- RH_AsientoProvisionLiquidacion
- GenerarAsistenciaFirmadosxFechas
- MCP_DesgloseCambioPremio
- LIQ_TraerNuevoMontoPlanPremios
- MCP_AsientoCambioPremios

El Departamento de Tecnologías de la Información, definió el estándar para la creación de procedimientos almacenados en la base de datos institucional de la siguiente manera:

> ***" c) Nombre de un procedimiento almacenado***
>
> *Se construirá de la siguiente manera:*
>
> *"**SP**"_"**M**"+<siglas del sistema>_<nombre procedimiento>*
>
> *Donde:*
>
> *SP = Procedimiento Almacenado por sus siglas en inglés, se debe escribir en mayúscula.*
>
> *M = Significa módulo y se escribe en mayúscula.*
>
> *Siglas del sistema: mínimo 2 letras y máximo de 6 letras, en mayúscula*
>
> *Nombre procedimiento: nombre significativo del procedimiento mínimo de 5 letras y máximo 20 letras, donde para cada primer letra de cada palabra que se utilice se escribe en mayúscula y el resto en minúscula de manera consecutiva.*

El procedimiento almacenado que valida una cuenta en el módulo de Cambio de Premios, debe llamarse:

Ejemplo: *SP_MCP_ValidarCuenta."*

Obsérvese que los procedimientos almacenados, listados anteriormente, no cumplen con los estándares previamente definidos.

El propósito de la asignación de estándares, garantiza la aplicación de un nivel mínimo de calidad en los sistemas de información, proporciona un enfoque consistente y un lenguaje común en entornos con múltiples equipos de desarrollo, tanto para personal interno como externo, consigue que los componentes de los sistemas de información sean más fáciles de entender y mantener y finalmente facilitan el proceso de introducción a nuevo personal o personal autsoursing. Todo esto redunda en un aprovechamiento del tiempo y de los recursos.

2.2.4. Creación de trigger.

Los *triggers* son pequeños programas que se asocian con tablas y se almacenan en la base de datos. Estos tienen como función principal, alertar a los programadores sobre restricciones o actividades especiales a la hora de intentar *agregar, borrar o actualizar* información en una base de datos, de tal manera que, si se ejecuta una acción incorrecta, el trigger presenta una alerta (mensaje en pantalla), indicando sobre dicha acción.

De acuerdo a una revisión realizada a 10 "trigger" creados en la base de datos de la institución, se logró determinar que existen dos de ellos que no cumplen con el estándar de nomenclatura definido por el Departamento de Tecnologías de la Información, que se debe utilizar a la hora de programarlos.

Los dos "trigger" que no cumplen con el estándar de programación son los siguientes:

- td_L20ARC
- PR_AgregarTran_Liquidacion

En lo que respecta al estándar en el nombre de los "trigger" de base de datos, el Departamento de Tecnologías de la Información definió el siguiente:

" d) Nombre de un trigger

Se construirá de la siguiente manera:

"tr"+<tipo de control>+<nombre significativo del trigger

Donde:

Tipo de control:

i. ***ins:*** *Inserción y Actualización*
ii. ***del:*** *Borrado*

iii. ***upd:*** *Actualización.*

Nombre significativo del trigger: mínimo de 5 letras y máximo 20 letras, donde para cada primer letra de cada palabra que se utilice se escribe en mayúscula y el resto en minúscula de manera consecutiva.

El trigger que valida una cuenta en el módulo de Cambio de Premios, debe llamarse:

Ejemplo: *trinsValidarCuenta"*

De acuerdo a lo anterior, los trigger indicados no cumplen con el estándar establecido para los mismos, por cuanto ninguno de los dos inicia con el "tr", no indican el "tipo de control" (insertar, borrar, actualizar), ni tienen un nombre significativo.

No aplicar el estándar en la confección de este tipo de programación (trigger) causa que los sistemas de información sean más difíciles de entender y mantener, sobre todo para las personas que se contraten en forma externa para el mantenimiento de los sistemas, máxime si no están familiarizadas en la forma en que el Departamento de Tecnologías de la Información lleva a cabo la programación.

2.3. Comprobación de la política relacionada con la gestión de acceso a los sistemas de información, bases de datos y servidores

Esta Auditoría al revisar la seguridad de los accesos a los servidores, determinó que si un mismo usuario ingresa a un servidor de desarrollo y a un servidor de producción simultáneamente, la información de ambos servidores interactúa, cuando lo correcto sería que cada servidor trabaje en forma independiente.

Para comprobar lo anterior, se procedió a efectuar la consulta de marcas de ingreso y salida del funcionario Wen Jie Zhen Wu, correspondientes a la primera quincena del mes de setiembre del 2016, en un servidor de producción y en un servidor de desarrollo, con ambas sesiones abiertas en forma simultánea, para lo cual se tomaron en consideración las siguientes condiciones:

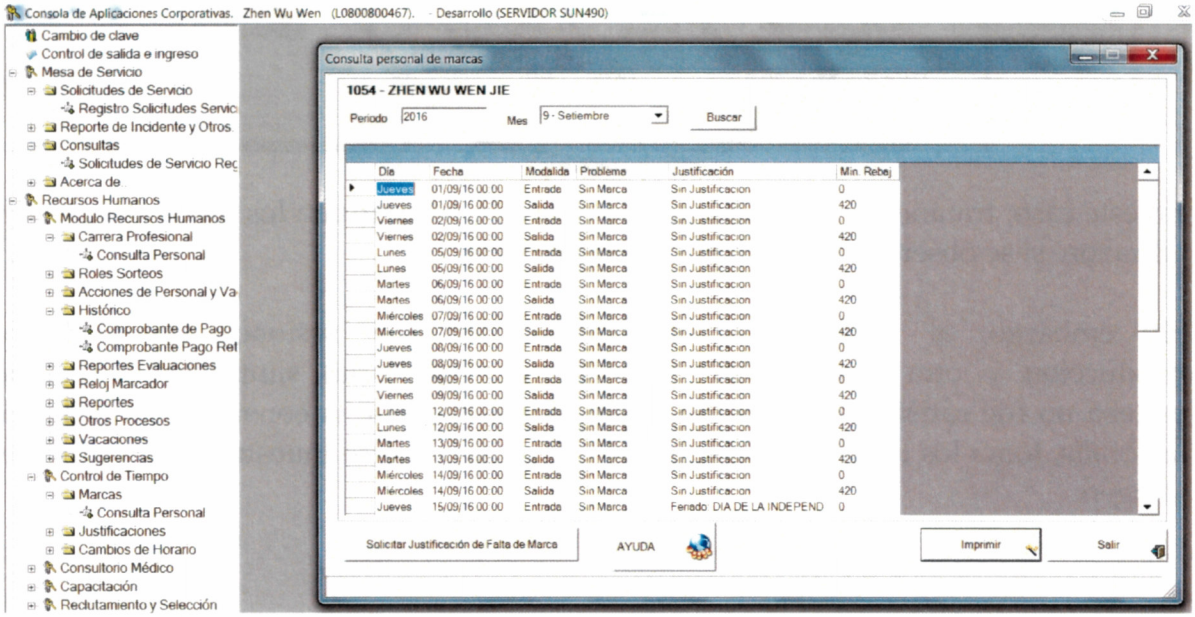
- Se utilizó el acceso a la Base de Datos de Producción (servidor 10.0.0.200) y el ejecutable de la consola de aplicaciones "sistemas.exe" (servidor 10.0.0.215).

- Se utilizó el acceso a la Base de Datos de Pruebas de Auditoría (servidor 10.3.0.4) y el ejecutable de la consola de aplicaciones (equipo local).

- Se procedió a utilizar el acceso a la consola "sistemas.exe" en el servidor de Producción y se creó una copia con el nombre "sistemaspruebas.exe" para acceder la Base de Datos de pruebas.

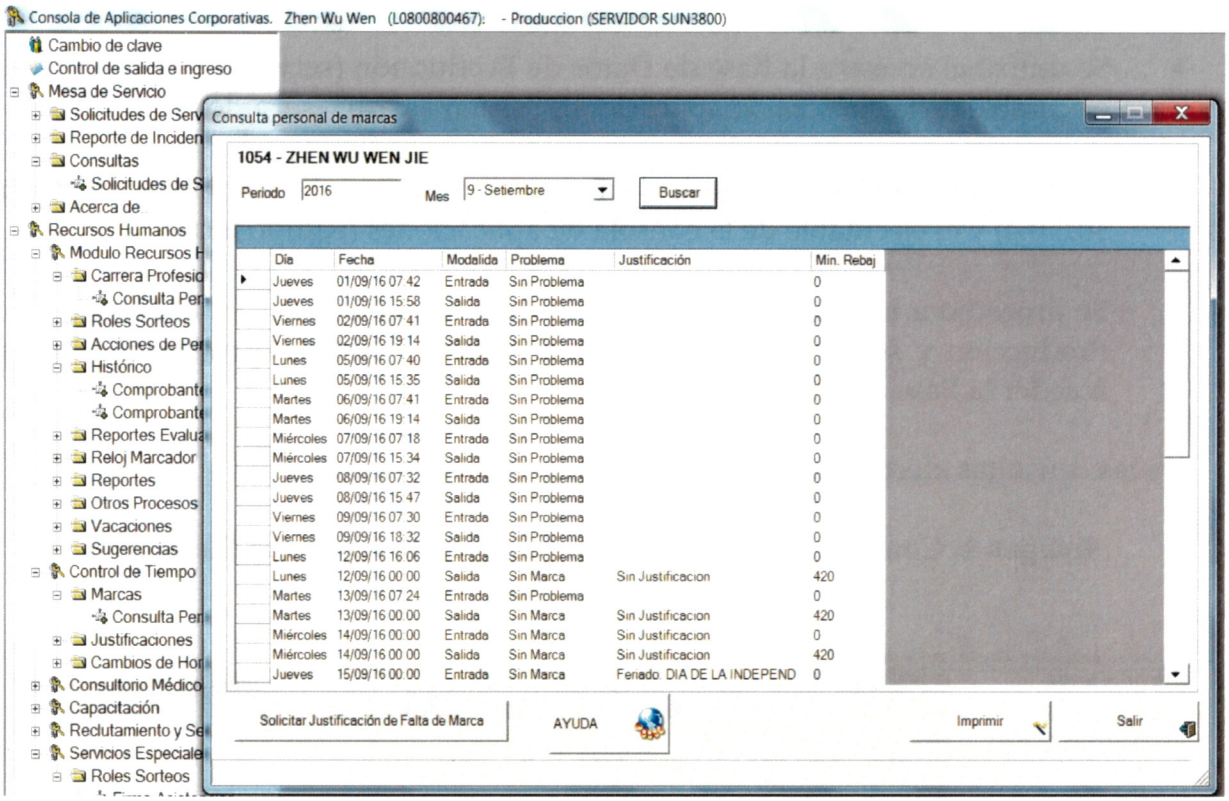
De las consultas efectuadas se obtuvieron los siguientes resultados:

Imagen 1. Consulta realizada en el servidor de la Auditoría (**Escenario Desarrollo**).



Observesé que por tratarse de un *ambiente de desarrollo*, no aparecen los datos reales de las marcas, por eso se muestra como si no exitieran las marcas de entrada ni de salida del funcionario.

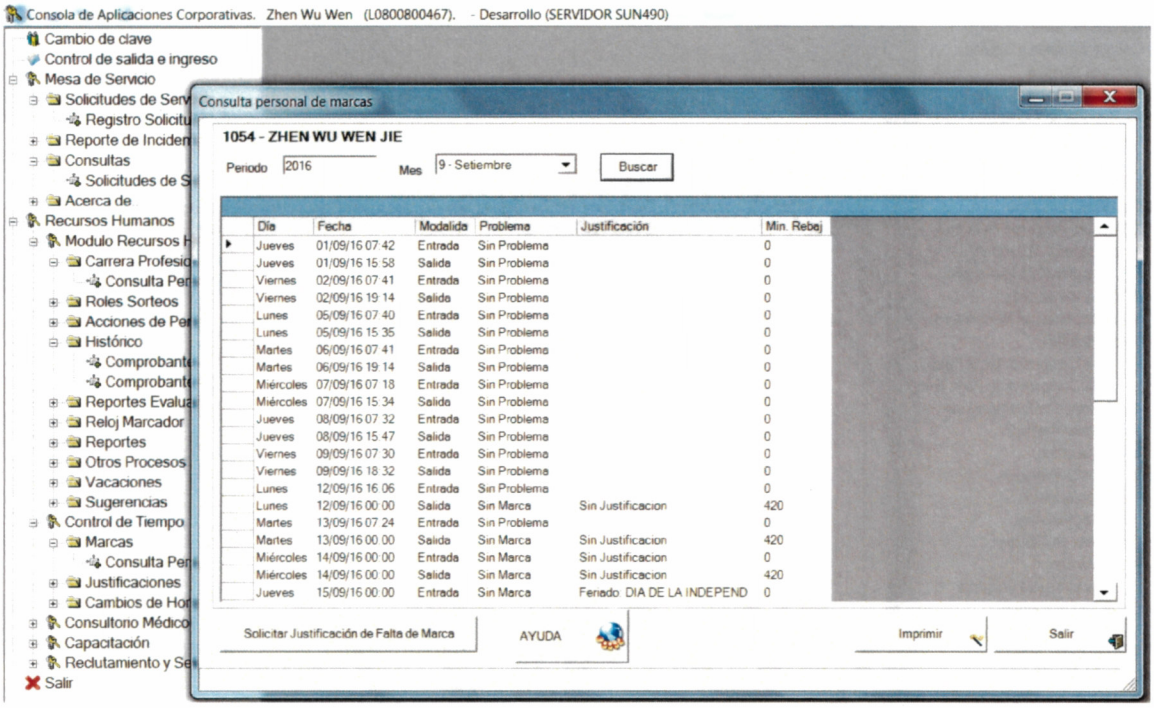
Imagen 2. Consulta realizada en el servidor de Producción.(**Escenario datos reales**)



En este caso, tratándose del *ambiente de producción*, sí aparecen los datos reales, por tal razón, sí se observan las marcas del funcionario.

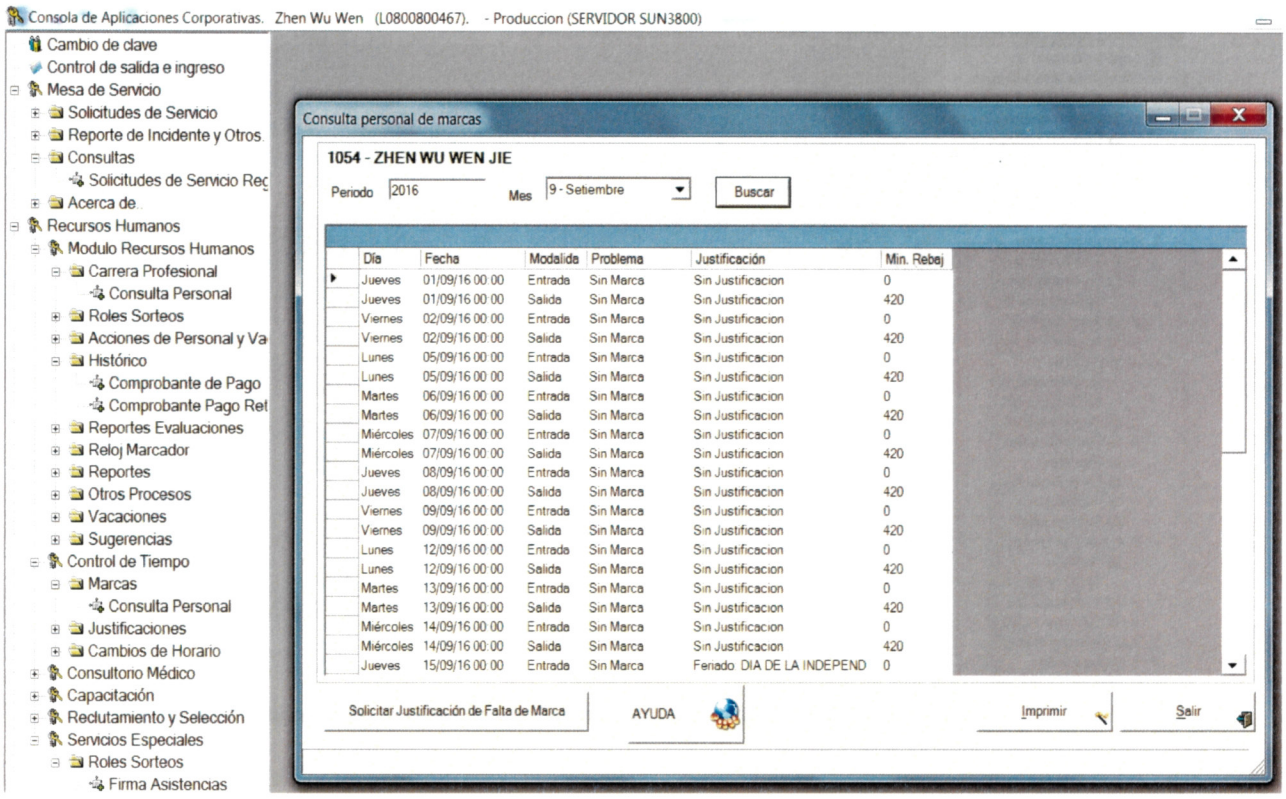
Sin embargo, al ingresar en un equipo, con dos sesiones abiertas una producción y otra a desarrollo (servidor de Auditoría) simultáneamente, la prueba no fue satisfactoria, debido a que el resultado de la consulta realizada en *desarrollo*, toma los datos de *producción* o viceversa como se muestra en la siguiente imagen:

Imagen 3. Consulta de datos en el **ambiente de desarrollo** (servidor de Auditoria), da como resultado los datos del servidor de producción.



La imagen anterior muestra que, estando en el *ambiente de desarrollo*, aparecen los datos del *ambiente de producción* (en este caso las marcas del funcionario), cuando lo correcto sería que éstas no aparezcan.

Imagen 4. Consulta en **ambiente de producción**



En esta imagen se puede observar que estando con la sesión abierta en el *ambiente de producción* no aparecen las marcas del funcionario, cuando lo correcto sería que sí se visualicen dichas marcas, por cuanto en ese ambiente, es en donde se almacenan los datos reales, tal como se mostró en la imagen 2.

Las Normas técnicas para la gestión y el control de las tecnologías de información, en la norma 1.4.6 referente a la "Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica", inciso c, indica:

> *"c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción."*

Aunque el Departamento de Tecnologías de la Información, mantiene los ambientes de desarrollo y producción separados, esta práctica se ve debilitada cuando un usuario accesa a ambos ambientes en forma simultánea.

El aspecto aquí detallado, podría eventualmente provocar, pérdida o cambio de información en los datos almacenados en la base de datos (integridad y seguridad), si se está laborando en ambiente de desarrollo y se tiene la sesión abierta en el ambiente de producción.

3. CONCLUSIONES.

El Departamento de Tecnologías de la Información, cuenta con un manual de políticas denominado *Manual Políticas de Administración Tecnologías de Información de Junta Protección Social*, este documento busca brindar un marco estratégico que regule las operaciones y servicios que proporciona la citada unidad, alineado a las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), emitidas por la Contraloría General de la República.

No obstante, en relación con los objetivos específicos planteados para este estudio y a criterio de esta Auditoría Interna, existen algunas políticas que no son cumplidas por el Departamento de Tecnologías de la Información, de lo cual podemos citar lo siguiente:

Dicha unidad administrativa no cuenta con un funcionario Encargado de Seguridad, con esta ausencia, no se están generando los informes mensuales de la labor de monitoreo de los accesos, lo cual puede traer como consecuencia la inobservancia de accesos no permitidos o usos indebidos de accesos previamente establecidos.

No se cuenta con un programa que encripte información confidencial, no toda la información debe estar encriptada, pero sí aquella considerada sensible para la institución, en este caso, el nivel de riesgo va en forma proporcional al tipo de información que se almacene en los equipos de los usuarios.

A la fecha de este informe, no se ha lanzado una campaña de concientización en materia de seguridad a los funcionarios de la Junta de Protección Social, lo cual es indispensable para que el personal conozca y tenga presente, las políticas referentes a la seguridad de la información, por cuanto es responsabilidad de todo el personal cumplir con los lineamientos establecidos en dichas políticas.

No se tiene una política para el manejo de datos históricos, la información histórica almacenada en una base de datos, consume gran cantidad de la capacidad de almacenamiento y el uso que se le dé a los mismos puede ser mínimo y en algunos casos nulo, lo que eventualmente demandarían un mayor tiempo de acceso a los datos que realmente están en uso.

No se están generando informes relacionados con la calidad de los servicios prestados por terceros al finalizar los contratos o al renovarlos, este monitoreo sería muy útil para conocer si la inversión en este tipo de contrataciones está dando el resultado esperado, igualmente si es procedente la continuación de los servicios.

El Departamento de Tecnologías de la Información, no es uniforme al aplicar el modelo de estándar de desarrollo y creación de base de datos, en lo que respecta a: la creación de columnas o campos (y sus nombres), en la creación de procedimientos almacenados y en la creación de trigger. El propósito de la asignación de estándares, es dar un enfoque consistente y un lenguaje común en entornos con múltiples equipos de desarrollo, tanto para personal interno como externo, asimismo, logra que los componentes de los sistemas de información sean más fáciles de entender y mantener, también facilitan el proceso de introducción a nuevo personal o personal autsoursing. Todo esto redunda en un aprovechamiento del tiempo y de los recursos.

Finalmente, se observó una debilidad de control cuando un desarrollador de sistemas se encuentra laborando en un servidor de desarrollo y tiene abierta simultáneamente la sesión en un servidor de producción, al darse esta situación la información de ambos servidores interactúa, lo que puede ocasionar, eventualmente, que la información contenida en la base de datos sea alterada por error.

Las políticas fueron creadas como normas fundamentales que deben regir aspectos de seguridad, calidad del servicio, control y monitoreo de los temas relacionados con las tecnologías de la información aplicadas en la Junta de Protección Social, si éstas no se cumplen, se estaría ante falta de controles que minimicen el riesgo, desmejora en los procesos relacionados con los sistemas de información, así como en la adopción de aquellas medidas necesarias para garantizar la seguridad de la información y el mejoramiento en los procesos.

4. RECOMENDACIONES.

Al Gerente General: girar instrucciones al señor Ronald Ortíz Méndez, Jefe del Departamento de Tecnologías de la Información, para que lleve a cabo lo siguiente:

4.1 Corregir el texto señalado en la Política I del *Manual Políticas de Administración tecnologías de información de Junta de Protección Social,* en el apartado 4.3.5 referente a la Seguridad de la Información, página 18, de tal manera que se aclare la diferencia entre las labores correspondientes al ambiente de producción y al ambiente de desarrollo. (Hallazgo N° 2.1.1)

4.2 En vista de que a la fecha el Departamento de Tecnologías de la Información, no tiene un *Encargado de Seguridad*, esta Auditoria recomienda que se designe a un funcionario de ese departamento, para que lleve a cabo las labores que se consideren de mayor relevancia en dicho puesto, con la finalidad de mejorar el control interno institucional. (Hallazgo N° 2.1.2)

4.3 Poner en práctica, la campaña de concientización en materia de seguridad, llevada a cabo por el señor Steve Calvo Cruz (asesor externo), de tal manera que los funcionarios de la Junta de Protección Social estén actualizados con los temas de seguridad informática. (Hallazgo N° 2.1.4).

4.4 Agregar al *Manual de Políticas de Administración Tecnologías de Información*, una política referente al manejo de datos históricos, con la finalidad de que sirva de guía para las personas encargadas de realizar la manipulación de los datos históricos. (Hallazgo N° 2.1.5)

4.5 Implementar un programa de encriptado para aquella información que se considere de alto valor o amerite un grado mayor de seguridad, de tal manera que se cumpla con la política respectiva. Para cumplir con esto, es necesario que el Departamento de Tecnologías de la Información coordine con el dueño del proceso qué información es considerada crítica y por consiguiente debe ser encriptada. (Hallazgo N° 2.1.3).

4.6 Cumplir con lo indicado en la Norma 4.6 *Administración de servicios prestados por terceros* de las *Nomas Técnicas para la gestión y el control de las tecnologías de la información*, en donde se indica que debe asignarse a un responsable que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados, de igual forma aplicar las guías de seguimientos a contratos con proveedores, recomendadas por la empresa Deloitte & Touche S.A., según Licitación Abreviada N° 2011LA-00024-PROV, promovida por el Departamento de Tecnologías de la Información. (Hallazgo N° 2.1.6).

4.7 Que emita una circular a los funcionarios del Departamento de Tecnologías de la Información, indicándoles la obligatoriedad de usar los estándares para el desarrollo de sistemas, en los siguientes procedimientos:

- En la nomenclatura en la creación del nombre de las tablas (Hallazgo 2.2.1).
- En la creación de columnas o campos de las tablas de la base de datos (Hallazgo 2.2.2).
- En la creación de procedimientos almacenados (Hallazgo 2.2.3).
- En la creación de triggers (Hallazgo 2.2.4).

Estos mismos estándares deben ser comunicados entre el personal que se contrate externamente para el desarrollo o mantenimiento de sistemas.

4.8 Advertir en forma escrita a los desarrolladores de sistemas, sobre el riesgo de control que existe, si trabajan en un mismo equipo con los ambientes de producción y desarrollo abiertos simultáneamente, ya que por error podrían acceder a ciertas opciones e ingresar datos en producción en forma errónea, lo que eventualmente podría alterar la información contenida en la base de datos institucional. (Hallazgo 2.3)

Realizado por:
Lic. Andrés Martínez Porras
Profesional II

Realizado por:
Lic. Wen Jie Zhen Wu
Profesional II

Revisado por:
Lic. José Wong Carrión
Jefe de Área

Aprobado por:
MBA. Rodrigo Carvajal Mora
Subauditor Interno