DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL

INFORME FINAL A.I.I Nº 16/2023

AUDITORÍA ESPECIALIZADA Y/O INTEGRAL

AUDITORÍA INFORMÁTICA

PERIODO DE REVISIÓN: AÑO 2023

FECHA DEL INFORME: DICIEMBRE 2023

Índice

DIRECCIÓN DE AUDITORIA INTERNA

INFORME FINAL A.I.I. Nº 16/2023

1.- ANTECEDENTES

En el marco de las actividades a ser ejecutadas, por esta Dirección de Auditoría Interna, conforme al Plan de Trabajo y su Cronograma Anual, aprobados por la Máxima Autoridad Institucional, por **Resolución SFP N° 524/2022** de fecha 07 de octubre de 2022 *"Por la cual se aprueba el Plan de Trabajo Anual, el Cronograma de Actividades y la Identificación y Plan de Gestión de Riesgo para el Ejercicio Fiscal 2023 de la Secretaría de la Función Pública"*. Se procederá a realizar la auditoría informática de acuerdo al Ítem N° 1 del apartado D- Auditorías especializadas y/o integral del Plan de Trabajo Anual 2023 de la Auditoría Interna Institucional.

La ley 7158 de fecha 23 de agosto de 2023 "Que crea el Ministerio de Economía y Finanzas", dispone la absorción de la Secretaría de la Función Pública, la cual, a partir de su vigencia, depende orgánicamente del Ministerio de Economía y Finanzas. El Viceministerio de Capital Humano y Gestión Organizacional sustituye y absorbe las funciones de la Secretaría de la Función Pública. Toda referencia legal y reglamentaria a la Secretaría de la Función Pública, se considerará realizada al Viceministerio de Capital Humano y Gestión Organizacional.

Conforme al artículo 11 de la Ley 7158/2023, la Unidad de Administración y Finanzas de la Secretaría de la Función Pública, se constituye en SUAF, y pasa a depender de la Unidad de Administración y Finanzas del Ministerio de Economía y Finanzas, mientras transcurra el proceso de transición, para garantizar la prestación y el funcionamiento normal e ininterrumpido de los servicios institucionales.

2.- ALCANCE

La revisión y análisis de los sistemas de información, los procedimientos y las políticas de seguridad vigentes en la institución.

Los procedimientos aplicados consistieron en la revisión de las documentaciones, visita in situ a al área de DGTIC con el fin de concluir sobre el grado de razonabilidad de seguridad de los sistemas de información institucional.

Es responsabilidad de la Dirección General de Tecnologías de la Información y la Comunicación (DGTIC) el contenido de la información suministrada.

Fueron ejecutadas las pruebas y técnicas de Auditoría considerando las Normas de Auditoría Generalmente Aceptadas y al Manual de Auditoría Gubernamental a fin de sustentar los resultados alcanzados.

3.- OBJETIVOS

- Que el Sistema de Información ofrezca un grado de seguridad razonable y satisfaga las necesidades de los usuarios.

4.- ASPECTO LEGAL

La revisión se ha efectuado considerando las Normas de Auditoría Generalmente Aceptadas, utilizando el marco de las siguientes reglamentaciones:

- La Ley 7158/23 "Que crea el Ministerio de Economía y Finanzas"
- La Ley N° 1535/99 de "Administración Financiera".
- Decreto N° 6234/2016 "Por el cual se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TIC) en la Gestión Pública, se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento".
- La Resolución CGR 583/2019 "Por la cual se actualiza el Manual de Auditoria Gubernamental (MAGU) para las Instituciones Públicas sujetas a la fiscalización y control de la Contraloría General de la República, y se deja sin efecto la Resolución CGR 146 del 25 de Marzo de 2019"
- Resolución CGR N° 377/2016 "Por la cual se adopta la Norma de Requisitos Mínimos para un Sistema de Control Interno del Modelo Estándar de Control Interno para Instituciones Públicas de Paraguay – MECIP: 2015"
- Resolución AGPE N° 290/2017 "Por la cual se abrogan las Resoluciones AGPE N° 23/2014; 323/2014; 435/2014; 421/2015; 211/2016 y se reglamenta el uso del Sistema Integrado de la Auditoría General del Poder Ejecutivo - SIAGPE, para su implementación en las Auditorías Internas Institucionales de los Organismos y Entidades dependientes del Poder Ejecutivo".
- La Resolución SFP N° 777/2019 "Por la cual se adopta el Manual de Auditoría Gubernamental que establece la Auditoría General del Poder Ejecutivo"
- Resolución SFP N° 279/2018 "Por la cual se aprueban el Manual de Políticas de Uso de los Bienes y Servicios Informáticos, las Políticas de Seguridad Informática y el Plan de Contingencia y Continuidad de Sistemas de la Secretaría de la Función Pública, dependiente de la Presidencia de la República".
- Resolución SFP N° 439/2018 "Por la cual se aprueba el Manual de Información Institucional de la Secretaría de la Función Pública, dependiente de la Presidencia de la República".
- Resolución MITIC N° 733/2019 "Por la cual se aprueba el modelo de Gobernanza de Seguridad de la Información"

5.- PROCEDIMIENTOS

- Verificar el status de los aplicativos y elementos de configuración institucionales, para confirmar su integridad y seguridad.

6.- DESARROLLO DEL TRABAJO

Como parte de las tareas, la Dirección General de Tecnología de la Información y Comunicación (DGTIC) ha remitido a la Dirección de Auditoría Interna Institucional las documentaciones solicitadas surgidas a partir de la visita in situ de ésta Auditoría al área de DGTIC.

El análisis realizado corresponde al diagnóstico y evaluación del área de DGTIC conforme a lo establecido en el Plan de Trabajo Anual y Cronograma de actividades establecidas al Periodo 2023.

A continuación, se exponen las observaciones y recomendaciones realizadas a partir de las evidencias y los hallazgos encontrados en el proceso de verificación y análisis.

7.- OBSERVACIONES Y RECOMENDACIONES

OBSERVACIÓN N° 1: **El área de TIC no cuenta con una estructura mínima para su efectivo funcionamiento**

El **Decreto N° 6234/2016** *"Por el cual se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y la Comunicación (TIC) en la Gestión Pública, se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento"* menciona en su Artículo 5° que *"el área de TIC deberá contar con una estructura mínima que le permita cumplir con sus funciones, pudiendo esta ser ampliada de acuerdo a las necesidades de cada institución. Dicha estructura contempla cuatro (4) áreas de trabajo: 1- Sistemas, 2- Infraestructura y Operaciones TIC, 3-Seguridad TIC y 4- Mesa de Ayuda, y adicionalmente un Staff Técnico y Administrativo"*.

Según el **Organigrama Institucional**, el área de TIC se encuentra conformada de la siguiente manera:

Dirección General de Tecnologías de la Información y la Comunicación

1) Dirección de Investigación y Desarrollo

- ✓ Departamento de Investigación, Análisis e Innovación
- ✓ Departamento de Desarrollo de TIC's
- ✓ Departamento de Calidad de Software

2) Dirección de Soporte y Mantenimiento

- ✓ Departamento de Soporte Técnico
- ✓ Departamento de Mantenimiento

En ese sentido, según el **Manual de Funciones y Perfiles** de la Institución, se observa que si bien existen Direcciones cuyas funciones se ocupan de las áreas de trabajo de "Sistemas" (Dirección de Investigación y Desarrollo) e "Infraestructura y Operaciones TIC" (Dirección de Soporte y Mantenimiento) actualmente no existen áreas de trabajo que se ocupen de la Seguridad TIC y Mesa de Ayuda, por tanto el área de TIC no cumple con lo establecido en el artículo de la normativa citada precedentemente, no cuenta con una estructura mínima necesaria para su efectivo funcionamiento.

RECOMENDACIÓN N° 1

Cumplir con lo establecido en la normativa vigente, realizar la revisión de la estructura de la Dirección General de Tecnologías de la Información y Comunicación (DGTIC) y adecuarlo a las necesidades de la institución.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC'S

La DGTIC ha enviado a la administración anterior y a la administración actual la propuesta estructural acorde a las exigencias del decreto 6234/2016, a fin de cumplir con la normativa, hasta la fecha no tenemos respuestas.

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC's, esta auditoría toma conocimiento y se ratifica en la observación. La DGTIC deberá continuar con los trámites y acciones pertinentes a fin de reiterar la propuesta estructural ante la administración actual y cumplir con la normativa vigente. Se solicita la elaboración de un Plan de Mejoramiento que refleje las acciones de mejora a ser realizadas.

OBSERVACIÓN N° 2: **La institución no cuenta con un área de Seguridad de la Información**

La **Resolución MITIC N° 733/2019** "*Por la cual se aprueba el Modelo de Gobernanza de Seguridad de la Información"* Anexo I, menciona que "*toda institución pública deberá contar un Área de Seguridad de la Información, el cual deberá posicionarse en la estructura organizativa de manera a reportar a la Máxima Autoridad Institucional. El área de Seguridad de la Información no debe depender del área de TIC y no sustituye al área de Seguridad TIC y/o otras áreas operativas (...)*"

En ese sentido, según el Organigrama, la Institución no cuenta con un área de **Seguridad de la Información** con dependencia directa a la Máxima Autoridad Institucional que se encargue de la seguridad de todos los activos de información en cuanto a su confidencialidad, integridad y disponibilidad, según lo establecido en la normativa.

RECOMENDACIÓN N° 2

Cumplir con el Modelo de Gobernanza de seguridad de la información conforme a lo establecido en la normativa vigente.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC´S

La DGTIC ha enviado a la administración anterior y a la administración actual la propuesta estructural acorde a las exigencias del decreto 6234/2016, a fin de cumplir con la normativa, en el cual existe un área de Seguridad de la Información que hasta la fecha no tenemos respuestas.

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC´s, esta auditoría toma conocimiento y se ratifica en la observación. La DGTIC deberá continuar con los trámites y acciones pertinentes a fin de reiterar la propuesta estructural ante la administración actual y cumplir con la normativa vigente. Se solicita la elaboración de un Plan de Mejoramiento que refleje las acciones de mejora a ser realizadas.

OBSERVACIÓN N° 3: **No existe un procedimiento documentado aprobado para la realización de copias de seguridad**

Las **Políticas de Seguridad Informática**,(PSI) aprobadas por *Resolución SFP N° 279/2018*, se constituyen en una herramienta institucional para hacer conciencia a los funcionarios de la institución sobre la importancia y la sensibilidad de la información y servicios críticos que permiten a la institución crecer y mantenerse como institución líder en invocación. Son una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información.

Las Políticas de Seguridad Informática contiene varios apartados, uno de ellos se encuentra relacionado al **Back up de base de datos** en el que se visualizan el objetivo del mismo, su proceso y los responsables de su ejecución, sin embargo, no se visualizan los procedimientos técnicos y la frecuencia para la realización de copias de seguridad.

Si bien el Director General del área ha mencionado que *"los procedimientos técnicos y la frecuencia quedan a criterio del Jefe del Departamento de Soporte Técnico pudiendo realizarse de forma diaria, semanal y mensual"* dichos procesos no se encuentran establecidos en un documento formal aprobado que se constituya a su vez en un instructivo o guía para el Manual de Procedimientos del área.

RECOMENDACIÓN N° 3

Realizar la justificación conforme a la observación emitida. Documentar y/o actualizar las políticas de seguridad informática en cuanto al establecimiento de la frecuencia de realización de copias de seguridad y los procedimientos técnicos que pudieran identificarse.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC'S

El procedimiento de copias de seguridad se encuentra aprobado en la Políticas de Seguridad Informática pagina 6 al 8, Aprobado por Resolución SFP N° 0279/2018 de fecha 09/05/2018, además el procedimiento en si se realiza con herramientas informáticas que se utilizan para las copias de seguridad y se establecen los meses, días y horas según la frecuencia aplicada de forma completo e incremental. Se remite 2 documentos ***a) Backup NubePy.pdf y b) EsquemaDeRespaldo.pdf***

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC's, esta Auditoría ha verificado las evidencias documentales presentadas y se ratifica en la observación. La DGTIC deberá realizar las acciones necesarias a fin de actualizar las Políticas de Seguridad Informática, a través de un acto administrativo formalmente aprobado, e incluir los siguientes procedimientos técnicos presentados por el área:

- *Backup de sistemas en la Nube*
- *Generación de respaldo de los servicios de base de datos de producción de los sistemas SICCA y XRE*

Las acciones a ser realizadas deberán ser presentadas en un Plan de Mejoramiento.

OBSERVACIÓN N° 4: **No existe un criterio aprobado formalmente que defina la información crítica a ser resguardada en el servidor de archivos (memoria institucional)**

Las Políticas de Seguridad Informática aprobada por Resolución SFP N° 279/2019 (Anexo II) menciona en el apartado de "**PSI- 2** Generación de Backup's de archivo de usuarios – Procedimiento" que *"los Directores Generales y Directores de cada una de las Direcciones de la Secretaría de la Función Pública decidirán cuáles son los productos relevantes generados en el área que deben ser respaldados en el servidor de archivos"*

Así mismo, la Norma de Requisitos Mínimos para un Sistema de Control Interno del MECIP menciona en el apartado "**C- Componente de Control de la Implementación – Principio: Gestión de la Información – Sistema de Información**" que la información debe ser *"...d) Protegida: se debe restringir el acceso a la información crítica de modo que sólo las personas autorizadas puedan acceder a ella. Para esto, se deben implementar mecanismos apropiados de clasificación de la información"*

En ese sentido, no existe un documento formalmente aprobado por la institución que identifique la información crítica de cada área a ser respaldada en el servidor de archivos, a fin de proteger la información generada y evitar que el resguardo de documentos sea por decisión arbitraria de los Directores Generales y Directores.

RECOMENDACIÓN N° 4

Cumplir con lo establecido en la Norma de Requisitos Mínimos para un Sistema de Control Interno del MECIP, se debe implementar mecanismos apropiados de clasificación de la información aprobados por acto administrativo para identificar la información crítica de cada área a ser respaldada en el servidor de archivos y documentar dicha clasificación para eventuales revisiones o auditorías.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC'S

No existe el mecanismo apropiado de clasificación de la información crítica para identificar de cada área a ser respaldada

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC's, esta auditoría se ratifica en la observación. La Institución, con el apoyo de la DGTIC, deberá identificar, definir y clasificar la información crítica generada por cada área, a través de un acto administrativo, a fin de proteger y resguardar adecuadamente la información relevante en el servidor de archivos y dar cumplimiento a la normativa. Incluir dichas acciones en un Plan de Mejoramiento.

OBSERVACIÓN N° 5: **No se visualiza un orden lógico para la ubicación y resguardo de la información en el servidor de archivos (memoria institucional)**

La Norma de requisitos mínimos para un Sistema de Control Interno del MECIP menciona en el apartado "**C- Componente de Control de la Implementación – Principio: Gestión de la Información – Sistema de Información**" que la información debe ser *"...a) Accesible: debe resultar sencillo obtener la información por cada área, de acuerdo a sus requerimientos de información. Los usuarios deben saber qué información está disponible y en qué sistema de información pueden acceder a ella"*

En ese sentido, se observa que el servidor de archivos institucional contiene alojados diversos documentos no clasificados, es decir, archivos no agrupados en carpeta y carpetas vacías, por tanto, no se visualiza un mecanismo apropiado de clasificación que permita un orden lógico de documentos emitidos por área a fin mantener la calidad de la información resguardada en el servidor y contribuir a una mejora de la accesibilidad de la información.

RECOMENDACIÓN N° 5

Se recomienda establecer un orden lógico de documentos por área a través de un mecanismo apropiado de clasificación para obtener la información de forma sencilla, mantener su calidad y optimizar su accesibilidad a fin de cumplir con lo establecido en la Norma de Requisitos Mínimos para un Sistema de Control Interno del MECIP.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC'S

El orden lógico de las carpetas o sub carpetas en el servidor de archivos la determina el encargado del proceso, vale decir, que el encargado de cada área trabaja, determina el lugar y la forma de clasificar o enumerar sus archivos en sus propios espacios asignados para el alojamiento de sus documentos. La DGTIC no es encargada de ordenar los archivos de otras dependencias, solo la de asegurar el acceso con su usuario acorde a su perfil y rol en el servidor de archivos.

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC's, esta Auditoría toma conocimiento y se ratifica en la observación. La DGTIC deberá establecer un criterio unificado para el ordenamiento lógico de carpetas/subcarpetas por área en el servidor de archivos, a través de un documento aprobado por acto administrativo, que sirva de parámetro y permita a los responsables de cada área seguir lineamientos y alojar sus documentos relevantes de respaldo de forma ordenada en la carpeta que le corresponda y facilite a su vez, el monitoreo de archivos por parte de la DGTIC y la tarea de control en auditorías posteriores.

Se recomienda incluir dichas acciones en un Plan de Mejoramiento a fin de dar cumplimiento a lo establecido en la Norma de Requisitos Mínimos MECIP.

OBSERVACIÓN N° 6: **Subsistemas del SICCA en estado de obsolescencia**

El **Sistema Integrado Centralizado de la Carrera Administrativa (SICCA)** es un sistema integrado cuya implementación fue aprobada por Decreto 1212/2014 y comprende los siguientes subsistemas: *a) Planificación y puestos de Trabajo b) Selección e Ingreso c) Movilidad laboral y promoción d) Evaluación del desempeño e) Capacitación f) Administración del legajo digital g) Remuneraciones h) procesos jurídicos y j) Desvinculaciones.* El SICCA tiene como objetivo la profesionalización de la función pública, razón por la cual se constituye en un facilitador de gestión para las Unidades de Gestión y Desarrollo de Personas (UGDP) que utilizan el sistema para el registro de todos los datos referentes al funcionario desde su ingreso a la función pública hasta su desvinculación, resultados de las evaluaciones de desempeño, promociones, sanciones administrativas, capacitaciones recibidas, los pagos y beneficios percibidos y sus demás datos personales, familiares, académicos y laborales, que obrarán en el legajo digital. (*Decreto 1212/2014, Art. 5°)*

El Plan Estratégico Institucional 2020-2024 con proyección al 2030, aprobado por *Resolución SFP N° 515/2020* constituye la herramienta que marca la ruta de la Institución, reuniendo los objetivos institucionales, con sus indicadores, metas, programas de acción y responsables, como producto de un proceso trabajado por área, socializado y acordado de manera participativa en mesas de trabajos con la colaboración de todo el plantel de funcionarios.

Contiene además, el cuadro de mando integral que permitirá realizar el seguimiento de los 24 objetivos estratégicos contemplados en el PEI, a su vez cada uno cuenta con sus respectivos indicadores de cumplimiento a mediano y largo plazo, enmarcados en 50 programas de acción, indicando la corresponsabilidad de las áreas misionales y de apoyo estratégico.

Uno de los objetivos estratégicos dentro de la perspectiva del fortalecimiento institucional es: *Fortalecer el Sistema de Control Interno, además de potenciar la gestión tecnológica mediante la simplificación de los procesos y la automatización de ellos, así como el fortalecimiento de equipamiento tecnológico.* El objetivo posee varios indicadores, entre ellos uno relacionado al **Porcentaje de sistemas implementados y funcionando en la institución** cuyo responsable de su cumplimiento es la Dirección General de Tecnologías de la Información y la Comunicación (DGTIC).

En ese contexto, y según las evidencias presentadas por la DGTIC y las propias palabras del Director General, se observa que en la actualidad 6 (seis) de los subsistemas del SICCA están inactivos debido a que se encuentran en estado de obsolescencia y, en consecuencia, no puede darse el cumplimiento efectivo y eficiente de los indicadores del mencionado objetivo estratégico institucional, existiendo inclusive riesgos de incumplimiento en el largo plazo.

Los Subsistemas inactivos son los siguientes: *a) Selección en Ingreso b) Movilidad laboral y promoción c) Evaluación del desempeño d) Capacitación e) Administración de legajo digital y f) Desvinculaciones.*

RECOMENDACIÓN N° 6

Realizar la justificación conforme a la observación emitida y realizar los trámites necesarios y las acciones pertinentes a fin de mantener activos los Sistemas Informáticos evitando la obsolescencia para dar cumplimiento a los objetivos institucionales.

DESCARGO DE LA DIRECCIÓN GENERAL DE TIC'S

El SICCA se encuentra en estado de obsolescencia con herramientas tecnológicas deprecadas y la infraestructura obsoleta, pues ya tienen aproximadamente 10 años de uso los equipos y en la actualidad los sistemas de software y hardware tienen como vida útil normal entre los 3 y 4 años aproximadamente.
Estos 4 últimos años desde la DGTIC se impulsó la gestión para el llamado de la renovación de los equipos y obtener un nuevo data center con nuevos equipos informáticos, pero no tuvimos éxito, pues la licitación cayó en protesta y no pudo culminarse.

OPINIÓN DE LA AUDITORIA INTERNA INSTITUCIONAL

Con relación al descargo presentado por la Dirección General de TIC's, esta auditoría toma conocimiento y se ratifica en la observación. La DGTIC deberá continuar con las gestiones necesarias y las acciones pertinentes ante la administración actual a fin de obtener el nuevo Data Center y la renovación de equipos informáticos. Se solicita la elaboración de un Plan de Mejoramiento que refleje las acciones de mejora a ser realizadas.

9.- INFORME Y RECOMENDACIONES FINALES

Con relación a los descargos recibidos de la Dirección General de Tecnologías de la Información y Comunicación, la Dirección de Auditoría Interna ha tomado conocimiento y emitido opinión sobre los mismos.

La Auditoría Interna recomienda fortalecer las acciones que hacen a la seguridad e integridad de la información institucional.

Se recomienda elaborar el Plan de Mejoramiento Institucional y presentar a la Auditoría Interna a más tardar dentro de 30 (treinta) días hábiles a partir de la recepción del informe final.

MINISTERIO DE ECONOMÍA Y FINANZAS
Firmado por **Jorge Chamorro**, Dir. Gral. Gabinete Viceministerio de Capital Humano y Gestión Organizacional

Rubén Eduardo Acuña Meza
Técnico de Auditoría Interna
Dirección de Auditoría Interna

Jorge Chamorro Correa
Encargado de Despacho
Dirección de Auditoría Interna.

GOBIERNO DEL PARAGUAY | MINISTERIO DE ECONOMÍA Y FINANZAS

VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL
DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL

DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL

INFORME FINAL A.I.I Nº 16/2023

AUDITORÍA ESPECIALIZADA Y/O INTEGRAL

AUDITORÍA INFORMÁTICA

"EVIDENCIAS Y HALLAZGOS"

PERIODO DE REVISIÓN: AÑO 2023

FECHA DEL INFORME: DICIEMBRE 2023

MINISTERIO DE ECONOMÍA Y FINANZAS * VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL * REPÚBLICA DEL PARAGUAY

TETÃ REMBIOKUAI SÃMBYHYHA SECRETARÍA DE LA FUNCIÓN PÚBLICA	Manual de Funciones y Perfiles Secretaría de la Función Pública	Código: SFP-2016 Versión: 01 | Aprobado por Resolución SFP N°0081/2016 Fecha de aprobación: 04/02/2016

Denominación del Puesto/Unidad 12. 01. 08. 01. 11. 01.	Dirección de Investigación y Desarrollo	Descripción Corta	DID

Cargo:	Director/a

Conducción Política		Producción para la Sociedad	3	Producción para la Administración Pública	2	Administración y Apoyo Interno	1

Finalidad del Puesto Misión	Planificar, coordinar y dirigir la investigación y el desarrollo tecnológico en el área TICs, entregando soluciones tecnológicas con alta disponibilidad capaces de brindar el soporte a los procesos de la Secretaría de la Función Pública.
Indicadores de cumplimiento	1. Sistemas Desarrollados e Implementados. 2. Sistemas con Mantenimientos

UBICACIÓN DEL PUESTO EN LA ORGANIZACIÓN

Nivel de Dependencia	Superior Funcional:
Orgánica Misional	Director/a General Tecnologías de la Información y la Comunicación

Superior Estructural:	Áreas bajo su responsabilidad
Director/a General Tecnologías de la Información y la Comunicación	Jefaturas de Departamentos

PERFIL REQUERIDO

COMPONENTE	MÍNIMOS REQUERIDOS	OPCIONALES DESEABLES
EXPERIENCIA LABORAL	Se requiere experiencia laboral bajo el siguiente criterio: **Experiencia Específica:** 4 años en cargos de Alta Gerencia (Instituciones del sector público o privado) **Experiencia General:** 5 años en el sector público o privado Además de la idoneidad necesaria para el ejercicio del cargo.	Experiencia General: 6 años, Instituciones del sector público o privado.
EDUCACIÓN FORMAL o ACREDITADA	Profesional Universitario egresado de las Carreras de Ingeniería Informática y/o Análisis de Sistemas Informáticos.	Postgrado, Diplomado, Especialización Administración Pública, Seguridad de Sistemas Informáticos, Auditoría de Sistemas Informáticos y otros relacionados al área.
PRINCIPALES CONOCIMIENTOS ACREDITADOS	Conocimientos específicos referentes a Seguridad Informática, Auditoría de Sistemas Informáticos, Alta Gerencia Pública. Cursos/Seminarios/Talleres y Eventos relacionados al Puesto de Trabajo.	Conocimientos sobre Política y Estrategia Institucional, Alta Gerencia Pública, Políticas de Gestión de Personas.
HABILIDADES	Habilidad analítica y toma de decisiones Manejo de herramientas informáticas/Programas. Habilidad Comunicacional en idiomas oficiales (Español, Guaraní) e Inglés. Habilidad mediática para enfrentar diversas situaciones. Negociación y Resolución de Conflictos	Habilidad comunicacional en lengua extranjera
COMPETENCIAS	Competencias requeridas 1. Compromiso con la Calidad del Trabajo. 2. Conciencia Organizacional. 3. Iniciativa. 4. Integridad. 5. Flexibilidad. 6. Autocontrol. 7. Trabajo en Equipo. 8. Responsabilidad	
RIESGOS Y CONDICIONES DE TRABAJO	Riesgos a la salud: Aptitud física y mental para actividades que demandan en forma constante presiones y toma de decisiones (alto) Riesgos laborales: Situaciones probables de tensión nerviosa por las responsabilidades del cargo y eventuales crisis que administrar. Pasible de stress laboral.	

MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL

	Esfuerzo físico requerido: Requiere esfuerzo intelectual muy alto y eventualmente físico. Ambiente de trabajo: Actividades en oficina, adecuadamente iluminada, climatizada para la recepción de personas.	
OBSERVACIONES	a) No hallarse en las inhabilidades e incompatibilidades previstas en la Ley N° 1626/2000. b) No poseer retiro voluntario o incentivado en los plazos previstos en las normativas vigentes. c) Otros criterios que la máxima autoridad institucional especifique y que se encuentren enmarcados en las normas legales vigentes	

FUNCIONES GENERALES DEL PUESTO

PLANIFICACIÓN del propio trabajo o el de otros	Planificar las actividades y tareas relacionadas a la investigación, innovación y desarrollo de sistemas de información ajustados a los requerimientos de la SFP.
DIRECCIÓN o coordinación del trabajo de dependientes directos o indirectos	Dirigir las actividades y tareas relacionadas a la investigación, innovación y desarrollo de sistemas de información ajustados a los requerimientos de la SFP.
EJECUCIÓN personal por parte del ocupante del puesto	Coordinar y supervisar las actividades y tareas relacionadas a la investigación, innovación y desarrollo de sistemas de información ajustados a los requerimientos de la SFP.
CONTROL y/o evaluación del trabajo propio o de dependientes	Controlar y evaluar las actividades relacionadas a la a la investigación, innovación y desarrollo de sistemas de información ajustados a los requerimientos de la SFP.
Otros	Otras actividades y tareas inherentes al puesto de trabajo, que sean solicitadas por el superior inmediato o la MAI, establecidas mediante acto administrativo de la SFP.

FUNCIONES ESPECIFICAS DEL PUESTO

1. Participar en la formulación del Plan Estratégico de Tecnologías de la Información y Comunicación, contribuyendo activamente en el diagnóstico y la detección de las necesidades existentes.
2. Coordinar y dirigir procesos de trabajo relacionados a investigación (TIC's), desarrollo y elaboración de diseños de mejoras en la infraestructura y en las aplicaciones tecnológicas de la SFP.
3. Coordinar la asistencia técnica interna (SFP) sobre problemas o incidencias detectadas en los sistemas informáticos.
4. Coordinar la elaboración de propuestas de innovaciones relacionadas a infraestructura, aplicaciones y sistemas informáticos que puedan generar eficiencia en la ejecución de los procesos de trabajo y provisión de servicios en la SFP.
5. Coordinar y dirigir el desarrollo de sistemas informáticos que cumplan con las exigencias tecnológicas necesarias para el logro de los objetivos que fueron planificados institucionalmente.
6. Coordinar y dirigir la ejecución de procesos de mantenimiento correctivo y evolutivo de los sistemas de información de la SFP para contar con sistemas integrados de información ajustado a los requerimientos de la SFP.
7. Presentar informes técnicos al Director/a General Tecnologías de la Información y la Comunicación, sobre las actividades y avances en el desarrollo de los sistemas, efectuados en forma interna o por terceros.
8. Dirigir procesos tendientes a mantener la operatividad de los entornos de desarrollo, prueba y producción, mediante tareas preventivas y correctivas en coordinación con responsables de la Dirección de Soporte y Mantenimiento.
9. Coordinar las capacitaciones para la utilización de nuevas tecnologías y sistemas informáticos.
10. Representar a la Institución en las actividades relacionadas al área de competencia por designación del superior inmediato.

MINISTERIO DE ECONOMÍA Y FINANZAS
VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL

	Manual de Funciones y Perfiles Secretaría de la Función Pública	Código: SFP-2016
TETÃ REMBIJOKUÁI / MINISTERIO DE LA FUNCIÓN PÚBLICA		Versión: 01 — Aprobado por Resolución SFP N°0081/2016
		Fecha de aprobación: 04/02/2016

Denominación del Puesto/Unidad 12. 01. 08. 01. 11. 02.	Dirección de Soporte y Mantenimiento	Descripción Corta	DSM

Cargo:	Director/a

Conducción Política		Producción para la Sociedad	3	Producción para la Administración Pública	2	Administración y Apoyo Interno	1

Finalidad del Puesto Misión	**Planificar, Coordinar y Dirigir las acciones que permitan asegurar la disponibilidad, integridad, seguridad de la infraestructura tecnológica para garantizar la continuidad de los servicios brindados por la SFP.**
Indicadores de cumplimiento	1. Servicios de Soporte y Mantenimiento 2. Incidencias resueltas (preventiva y correctiva)

UBICACIÓN DEL PUESTO EN LA ORGANIZACIÓN

Nivel de Dependencia	Superior Funcional:
Orgánica Misional	Director/a General Tecnologías de la Información y la Comunicación

Superior Estructural:	Áreas bajo su responsabilidad
Director/a General Tecnologías de la Información y la Comunicación	Jefaturas de Departamentos

PERFIL REQUERIDO

COMPONENTE	MÍNIMOS REQUERIDOS	OPCIONALES DESEABLES
EXPERIENCIA LABORAL	Se requiere experiencia laboral bajo el siguiente criterio: **Experiencia Específica:** 4 años en cargos de Alta Gerencia (Instituciones del sector público o privado) **Experiencia General:** 5 años en el sector público o privado Además de la idoneidad necesaria para el ejercicio del cargo.	Experiencia General: 6 años, instituciones del sector público o privado.
EDUCACIÓN FORMAL o ACREDITADA	Profesional Universitario egresado de las Carreras de Ingeniería Informática y/o Análisis de Sistemas Informáticos.	Especialización y Maestría en materias: Administración Pública, Gestión de Personas, Finanzas Públicas, Desarrollo Humano, Presupuesto Público y otros relacionados al puesto de Alta Dirección
PRINCIPALES CONOCIMIENTOS ACREDITADOS	Conocimientos específicos referentes a Seguridad Informática. Conocimientos específicos en TIC' s. Conocimientos específicos de Gestión de la Calidad. Cursos/Seminarios/Talleres y Eventos relacionados al Puesto de Trabajo.	Auditoría de Sistemas Informáticos, Conocimientos sobre Política y Estrategia Institucional, Derecho Administrativo, Políticas de Gestión de Personas
HABILIDADES	Habilidad para el manejo de herramientas Tics. Habilidades analíticas y toma de decisiones. Habilidad Comunicacional en idiomas oficiales (Español, Guaraní). Habilidad mediática.	Habilidad comunicacional en lengua extranjera
COMPETENCIAS	Competencias requeridas 1. Compromiso con la Calidad del Trabajo. 2. Conciencia Organizacional. 3. Iniciativa. 4. Integridad. 5. Flexibilidad. 6. Autocontrol. 7. Trabajo en Equipo. 8. Responsabilidad	
RIESGOS Y CONDICIONES DE TRABAJO	<u>Riesgos a la salud</u>: Aptitud física y mental para actividades que demandan en forma constante presiones y toma de decisiones	

MINISTERIO DE ECONOMÍA Y FINANZAS — VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL

	(moderado) Riesgos laborales: Situaciones probables de tensión nerviosa por las responsabilidades del cargo. Pasible de stress laboral. Esfuerzo físico requerido: Requiere esfuerzo intelectual alto y eventualmente físico. Ambiente de trabajo: Actividades en oficina, adecuadamente iluminada, climatizada para la recepción de personas.	
OBSERVACIONES	a) No hallarse en las inhabilidades e incompatibilidades previstas en la Ley N° 1626/2000. b) No poseer retiro voluntario o incentivado en los plazos previstos en las normativas vigentes. c) Otros criterios que la máxima autoridad institucional especifique y que se encuentren enmarcados en las normas legales vigentes	

FUNCIONES GENERALES DEL PUESTO

PLANIFICACIÓN del propio trabajo o el de otros	Planificar las actividades y tareas relacionadas a los procesos de TIC's para asegurar la disponibilidad, confidencialidad, integridad y seguridad de la infraestructura tecnológica.
DIRECCIÓN o coordinación del trabajo de dependientes directos o indirectos	Dirigir las actividades y tareas relacionadas a los procesos de TIC's para asegurar la disponibilidad, confidencialidad, integridad y seguridad de la infraestructura tecnológica.
EJECUCIÓN personal por parte del ocupante del puesto	Coordinar y supervisar las actividades y tareas relacionadas a los procesos de TIC's para asegurar la disponibilidad, confidencialidad, integridad y seguridad de la infraestructura tecnológica.
CONTROL y/o evaluación del trabajo propio o de dependientes	Controlar y Evaluar las actividades y tareas relacionadas a los procesos de TIC's para asegurar la disponibilidad, confidencialidad, integridad y seguridad de la infraestructura tecnológica.
Otros	Otras actividades y tareas inherentes al puesto de trabajo, que sean solicitadas por el superior inmediato o la MAI, establecidas mediante acto administrativo de la SFP.

FUNCIONES ESPECIFICAS DEL PUESTO

1. Planificar y Dirigir la ejecución de actividades a fin de garantizar la disponibilidad de la plataforma tecnológica de la SFP y sus dependencias.
2. Supervisar la elaboración y ejecución del plan anual de mantenimiento preventivo de la infraestructura tecnológica de la SFP.
3. Prever y definir los requerimientos tecnológicos futuros para la adquisición de la infraestructura TIC's de la SFP.
4. Dirigir la administración y monitoreo de la ejecución de la tareas de respaldo de datos y servicios de tecnología y comunicación de la SFP.
5. Supervisar el cumplimiento y la actualización de las políticas y normativas de seguridad en materia de TIC's.
6. Controlar el inventario del parque tecnológico de la SFP, a fin de llevar un control de la vigencia de la garantía.
7. Planificar la adquisición y renovación de licencias, certificados, firma digital, delegación de dominios, firmware, suscripciones y registros de marcas.
8. Planificar la capacitación del personal técnico para asegurar la calidad de los servicios en la institución.
9. Participar en la formulación del Plan Estratégico de Tecnologías de la Información y Comunicación, contribuyendo activamente en el diagnóstico y la detección de las necesidades existentes.
10. Representar a la institución en las actividades relacionadas al área de competencia por designación del superior inmediato.

MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL

PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY
MINISTERIO DEL INTERIOR

DECRETO Nº 2944

POR EL CUAL SE APRUEBA LA ESTRUCTURA ORGÁNICA DE LA SECRETARÍA DE LA FUNCIÓN PÚBLICA (SFP), DEPENDIENTE DE LA PRESIDENCIA DE LA REPÚBLICA.

I. *Nivel de Conducción Política:*

Ministro Secretario Ejecutivo
- *a. Dirección de Secretaría Privada*
- *b. Asesorías Técnicas.*

II. *Nivel de Dependencias Estratégicas y Orgánicas de Apoyo:*

- *a. Coordinación MECIP.*
- *b. Dirección de Auditoría Interna Institucional.*
- *c. Secretaría General.*
- *d. Dirección de Gestión y Desarrollo de las Personas.*
- *e. Dirección General de Gabinete:*
  - *i. Dirección de Cooperación Internacional y Proyectos.*
  - *ii. Dirección de Transparencia y Anticorrupción.*
- *f. Dirección General de Administración y Finanzas:*
  - *i. Dirección de Finanzas.*
  - *ii. Dirección Operativa de Contrataciones.*
- *g. Dirección General de Comunicación Estratégica:*
  - *i. Dirección de Información y Comunicación Pública.*
- *h. Dirección General de Planificación y Monitoreo:*
  - *i. Dirección de Políticas de Inclusión y no Discriminación.*
  - *ii. Dirección de Planificación y Evaluación.*

III. *Nivel de Dependencias Orgánicas Misionales:*

- *a. Dirección General Tecnologías de la Información y la Comunicación (TIC):*
  - *i. Dirección de Investigación y Desarrollo.*
  - *ii. Dirección de Soporte y Mantenimiento.*
- *b. Dirección General de Concursos:*
  - *i. Dirección de Perfiles y Competencias.*
- *c. Dirección General de Asesoramiento Técnico a Organismos y Entidades del Estado (OEE):*
  - *i. Dirección de Desarrollo Institucional.*
  - *ii. Dirección de Asistencia Técnica Legal.*

Dirección de Decretos y Leyes
Secretaría General
Gabinete Civil

MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE CAPACITACIÓN Y GESTIÓN ORGANIZACIONAL

PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY
MINISTERIO DEL INTERIOR

DECRETO N° 2944.

POR EL CUAL SE APRUEBA LA ESTRUCTURA ORGÁNICA DE LA SECRETARÍA DE LA FUNCIÓN PÚBLICA (SFP), DEPENDIENTE DE LA PRESIDENCIA DE LA REPÚBLICA.

-4-

d. Dirección General del Instituto Nacional de la Administración Pública del Paraguay (INAPP):
i. Dirección Académica.

e. Dirección General de Asuntos Jurídicos;
i. Dirección de Producción y Control Normativo.
ii. Dirección de Sumarios Administrativos.

Art. 2°.- *Derógase el Decreto N° 4067 del 17 de marzo de 2010, "Por el cual se aprueba la Reestructuración Orgánica y Funcional de la Secretaría de la Función Pública, dependiente de la Presidencia de la República".*

Art. 3°.- *Establécese que la organización estructural y funcional de las dependencias citadas en este Decreto, serán definidas y aprobadas por Resolución de la Secretaría de la Función Pública, dependiente de la Presidencia de la República.*

Art. 4°.- *El presente Decreto será refrendado por el Ministro del Interior.*

Art. 5°.- *Comuníquese, publíquese e insértese en el Registro Oficial.*

N°

Dirección de Decretos y Leyes
Secretaría General
Gabinete Civil
www.presidencia.gov.py

MINISTERIO DE ECONOMÍA Y FINANZAS
MINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL

POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)

PSI -1 Backup's de Base de Datos

Descripción

Backup de respaldo de las bases de datos institucionales para continuidad del servicio.

Objetivo

Mantener un backup actualizado de contingencia de todas las bases de datos institucionales en sitio alternativo.

Procedimiento

1) Mantenimiento de la configuración de la tarea programada (CRON) que genera el backup de cada una de las bases de datos del entorno de producción.
2) Verificación del alojamiento exitoso del archivo de backup en sitio alternativo, que el proceso de la noche haya finalizado satisfactoriamente.
3) En caso de resultado fallido del procedimiento 2), previsión del traslado físico del backup.

En todos los casos se debe realizar la prueba de restauración del backup cada 48 horas para la verificación de la validez del backup.

El responsable

1. De la ejecución del proceso de backup, el Jefe del Departamento de Soporte Técnico (Interno 2038)
2. De las pruebas de restauración del backup, el Jefe del Departamento de Desarrollo TIC's. (Interno 2034)

El acceso a los archivos de backup's estará restringido y se permitirá únicamente a los dos Jefes de Departamentos mencionados.

PSI – 2 Generación de backup's de archivos de usuarios

Descripción

Backup de respaldo de información sensible generado por los funcionarios en sus respectivos equipos de cómputo.

Objetivo

Mantener un backup actualizado de contingencia de la información relevante existente en documentos de texto, planillas electrónicas, diapositivas de presentaciones, materiales audiovisuales y cualquier otro tipo de trabajo producido para el cumplimiento de sus funciones.

Procedimiento

1) Los Directores Generales y Directores cada una de las Direcciones de la Secretaría de la Función Pública decidirán cuáles son los productos relevantes generados en el área que deben ser respaldados en el servidor de archivos.
2) Los archivos a ser guardados en el servidor de archivos no deben incluir información personal del usuario, solamente la información producida para el cumplimiento de sus funciones en la SFP.
3) Cada usuario deberá mantener en su equipo de cómputo la información original, siendo una copia de contingencia la guardada en el servidor de archivos.
4) El usuario es el responsable de la información guardada en el servidor de archivos.
5) La ausencia de la copia de respaldo en el servidor de archivos, será responsabilidad del usuario.
6) La violación del procedimiento 2) será notificada al superior del área por primera vez, la reincidencia será comunicada a la MAI.
7) El Jefe del Departamento de Soporte Técnico está autorizado a realizar monitoreo periódico de los archivos guardados en el servidor de archivos.

El responsable

1. El usuario es el responsable de mantener la copia actualizada de sus datos relevantes en el servidor de archivos.
2. El monitoreo e Informe sobre la violación del procedimiento 2) estará a cargo únicamente para el Jefe de Soporte Técnico (Interno 2038).

PSI – 3 Seguridad perimetral o física

Descripción

Acceso físico al Data center y seguridad de los equipos de cómputo asignados a los usuarios.

Objetivo

Mantener la seguridad física del data center, todo lo referido a los equipos informáticos y equipamiento de red, todo con el fin de mitigar eventuales ataques internos o externos.

Procedimiento

1) La restricción del acceso físico al área del data center por parte de personas ajenas al Departamento de Soporte Técnico. Se encuentra vigente la Resolución SFP Nº 278/2014 por la cual se Reglamenta el acceso y la permanencia de Personas (Art.3°).

2) Prohibición de abrir las PCs y/o manipular por parte del usuario, sólo está autorizado el personal de soporte técnico.

   La violación del procedimiento 2) será notificada al superior del área por primera vez, la reincidencia será comunicada a la MAI.

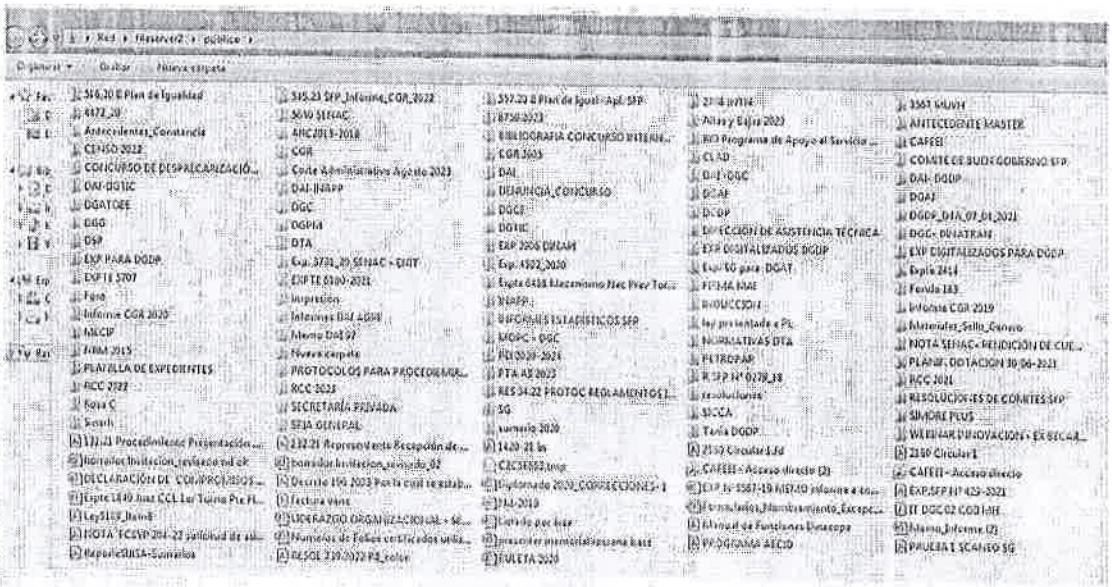
3) Si por razones de servicio, es necesario prestar equipos informáticos (computadoras portátiles tipo notebook) u otro tipo de equipo informático para ser utilizado en alguna presentación o evento, es obligatorio registrar en el libro de entrada/salida de equipos informáticos, fecha de retiro, fecha de devolución, firma y aclaración de nombres y apellidos.

0000020

0000018

VISUALIZACIÓN DEL SERVIDOR DE ARCHIVOS INSTITUCIONAL (CARPETA PÚBLICA)

Fecha de Captura: *15/12/2023*



8. Perspectivas/Objetivos Estratégicos PEI 2020-2024

En el PEI 2015-2019, se establecieron cuatro Perspectivas, como resultado de los talleres llevados a cabo y conforme la consulta virtual se ha acordado incluir dos perspectivas más, de esta forma las Perspectivas para el PEI 2020-2024 serían:

1ª. Del Funcionariado
2ª. De los Organismos y Entidades del Estado (OEE)
3ª. De la Ciudadanía
4ª. Del Fortalecimiento Institucional de la SFP
5ª. De Aprendizaje, Investigación, Desarrollo e Innovación
6ª. De Coordinación y Articulación Intersectorial/Interinstitucional

La definición de cada una de estas perspectivas son las siguientes:

1ª. PERSPECTIVA DEL FUNCIONARIADO

Objetivos Estratégicos

1. Consolidar el proceso de igualdad, equidad, idoneidad y oportunidad para el acceso y promoción en la función pública de forma transparente.
2. Promover e implementar un proceso de capacitación y formación de los/as servidores/as públicos.
3. Promoción de garantías y derechos laborales de las/os servidoras/es públicos.

2ª. PERSPECTIVA DE LOS ORGANISMOS Y ENTIDADES DEL ESTADO

Objetivos Estratégicos

1. Promover e implementar un proceso de formación y capacitación para Organismos y Entidades del Estado (OEE).
2. Mejorar la gestión y el desarrollo de las personas en los OEE.
3. Disponibilizar de manera transparente y de fácil acceso la información sobre el funcionariado y el uso de los recursos públicos de las OEE.
4. Fortalecer la gestion de expedientes internos y externos, así como la comunicación oficial de la SFP.
5. Fortalecer la descentralización de servicios provcidos por la SFP.

3ª. PERSPECTIVA DE LA CIUDADANÍA

Objetivos Estratégicos

1. Fortalecer la comunicación institucional tanto interna como externa.
2. Promover la participación de la ciudadanía en la gestión de los servicios públicos, a través del conocimiento y acceso a la información, por medio de tecnologías de información y comunicación (TIC's) y otras formas de comunicación.

4ª. PERSPECTIVA DEL FORTALECIMIENTO INSTITUCIONAL DE LA SFP

Objetivos Estratégicos

1. Fortalecer la autonomía institucional a través de la gestión de recursos propios y el ajuste normativo.
2. Gestión óptima de recursos humanos con las competencias conforme a la estructura organizacional y funcional, así como la adecuación de la infraestructura edilicia acorde a una planificación de crecimiento institucional.
3. Fortalecer el Sistema de Control Interno, además de potenciar la gestión tecnológica in-

diante la simplificación y automatización de procesos, así como el fortalecimiento de la infraestructura tecnológica.

4. Potenciar los procesos de descentralización de los servicios de capacitación y asistencia técnica por la SFP.

5°. PERSPECTIVA DE APRENDIZAJE, INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

Objetivos Estratégicos

1. Gestión basada en procesos.
2. Gestión del Conocimiento.

6°. PERSPECTIVA DE COORDINACIÓN Y ARTICULACIÓN INTERSECTORIAL/ INTERINSTITUCIONAL

Objetivos Estratégicos

1. Establecer convenios y desarrollar alianzas estratégicas.
2. Fortalecer la gestión de la comunicación institucional, interinstitucional e intersectorial.
3. Promoción de Garantías y Derechos Laborales de las/os Servidores/es Públicos.

OBJETIVOS	INDICADORES	Metas		PROGRAMAS DE ACCIÓN	RESPONSABLES
		Mediano	Largo		
	Porcentaje de cumplimiento de Plan de Mejora en materia de reglamento interno, manual de funciones, estructura y organigramas.	50%	100%	Plan de Mejoramiento de la SFP.	Dirección General de Asesoramiento Técnico a OEE, Dirección de Gestión y Desarrollo de las Personas, Dirección de Auditoría SFP, Dirección General de Planificación Estratégica
OE4.3. Fortalecer el Sistema de Control Interno, además de potenciar la gestión tecnológica mediante la simplificación de los procesos y automatización de ellos, así como el fortalecimiento de equipamiento tecnológico	Porcentaje de avance en la implementación del MECIP	70%	100%	Plan de Trabajo Instalación MECIP 2015	Áreas Misionales, Estratégicas y de Apoyo de la SFP Dirección General de Asuntos Jurídicos
	Porcentaje de Sistemas implementados y funcionando en la SFP. Grado implementación plan TICS.	50%	100%	Plan Maestro de TICS Plan Estratégico de TICS Plan de Mejoras del IGP para la SFP	Dirección General de Tecnologías de la Información y la Comunicación Dirección General de Comunicación Estratégica
	Porcentaje de OEE que aplican Sistemas de Gestión de la SFP, a través de plataformas tecnológicas.	50%	100%		
	Grado de cumplimiento del plan de mejoras, como resultado de aplicación IGP	50%	100%		
	Porcentaje de incremento del número de acciones, identificadas como buenas prácticas (formación del capital humano en áreas clave como la gestión documental, innovación, aprendizaje, diseño y uso de herramientas en TIC), respecto al año anterior.	20%	30%		

DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL

INFORME FINAL A.I.I Nº 16/2023

AUDITORÍA ESPECIALIZADA Y/O INTEGRAL

AUDITORÍA INFORMÁTICA

"DOCUMENTOS REFERENTES AL DESCARGO DE LA DGTIC"

PERIODO DE REVISIÓN: AÑO 2023

FECHA DEL INFORME: DICIEMBRE 2023

Backup Nube

Esquema General

A continuación se describe el esquema de backup utilizado para realizar el backup de los sistemas que se encuentran en la nube.

- Cada una de las máquinas virtuales que tienen sistemas en producción en la nube py tiene un usuario backup.
- El usuario backup es el encargado de realizar los backup de los sistemas que tiene alojado cada máquina virtual.
- En cada una de las máquinas virtuales de la nube existe una carpeta /backup donde se encontrará el script que realiza el backup de los sistemas y todos los archivos que son generados por el script de backup.
- Todos los scripts están automatizados con el crontab de cada máquina virtual para el usuario backup.
- Cada script de backup de cada máquina virtual borra el backup actual local y crea un nuevo backup con la fecha del día en que se ejecuta el script.
- En la virtual 192.168.1.10 (acceso) se encuentra configurada una tarea automática (crontab) con el usuario backup que copia, en la carpeta /backup, todos los backups que se encuentran en las demás máquinas virtuales. El copiado lo realiza de la siguiente manera:
    - Copia los backup de los sistemas dentro de la carpeta /backup de la virtual 192.168.1.10 en carpetas nombradas con el último número de la IP de cada máquina virtual.
    - Realiza el copiado de todos los backups recogidos al servidor de backup de la SFP que se encuentra en la red interna de la SFP (10.1.40.205) en la carpeta /nube_backup donde para cada virtual de la nube se encuentra una carpeta nombrada con el último número de la IP de la virtuales.
    - Cuando termina el copiado al servidor de backup de la SFP, se realiza el borrado de todos los archivos del virtual acceso, dejando el historial de backup de los sistemas de la nube en el servidor de backup de la SFP en la carpeta /nube_backup.

Configuraciones

Para realizar el esquema de backup se realizaron las siguientes configuraciones:

En la virtual 192.168.1.10 se configuró la clave pública privada de la siguiente manera:

Con el usuario backup, se ingresó a la carpeta /home/backup y se creó la carpeta oculta .ssh. Dentro de esta carpeta se ejecutó el comando ssh-keygen -t dsa y luego se presionó tres veces enter para setear nombres y contraseñas por defecto.

Este comando generó dos archivos: id_dsa.pub y id_dsa. El archivo id_dsa.pub corresponde a la clave pública y el archivo id_dsa corresponde a la clave privada.

En cada una de las virtuales que alojan los sistemas y en el servidor de backup de la SFP se realizó lo siguiente:

Con el usuario backup, se ingresó a la carpeta /home/backup y se creó la carpeta oculta .ssh. Dentro de esta carpeta se ejecutó lo siguiente:

chmod 700 ~/.ssh

cd ~/.ssh

touch authorized_keys

chmod 600 authorized_keys

En el archivo authorized_keys se copio el contenido del archivo id_dsa.pub de la virtual 192.168.1.10

Consideraciones a tener en cuenta en cada maquina virtual que alojan sistemas

Archivo /etc/ssh/sshd_config

- Se debe asegurar que si se tiene configurado el AllowUsers, se debe agregar una entrada para el usuario backup
- Se debe descomentar la línea AuthorizedKeysFile .ssh/authorized_keys

Archivo /etc/hosts

- Se debe tener la entrada acceso.sfp.gov.py

Archivo /etc/hosts.allow

- Se debe tener la entrada para la IP 192.168.1.10 y en el servidor de backup de la SFP se debe tener la entrada para la IP 10.2.79.133.

En todas las máquinas debe estar instalado el rsync

MINISTERIO DE ECONOMÍA Y FINANZAS

Firmado por **Juan Aguilera,**
Dir. Gral. TIC
Viceministerio de Capital Humano y Gestión Organizacional

MINISTERIO DE ECONOMÍA Y FINANZAS * VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL * REPÚBLICA DEL PARAGUAY

0000027

SECRETARÍA DE LA FUNCIÓN PÚBLICA

Dirección General de Tecnología de la Información y Comunicación

Departamento de Mantenimiento

Objetivo:

Detallar el proceso de generación de respaldo de los servicios de bases de datos de producción de los sistemas SICCA y XRE.

Especificar los pasos realizados para la transferencia automatizada de los archivos generados desde los servidores asociados al servidor de respaldo.

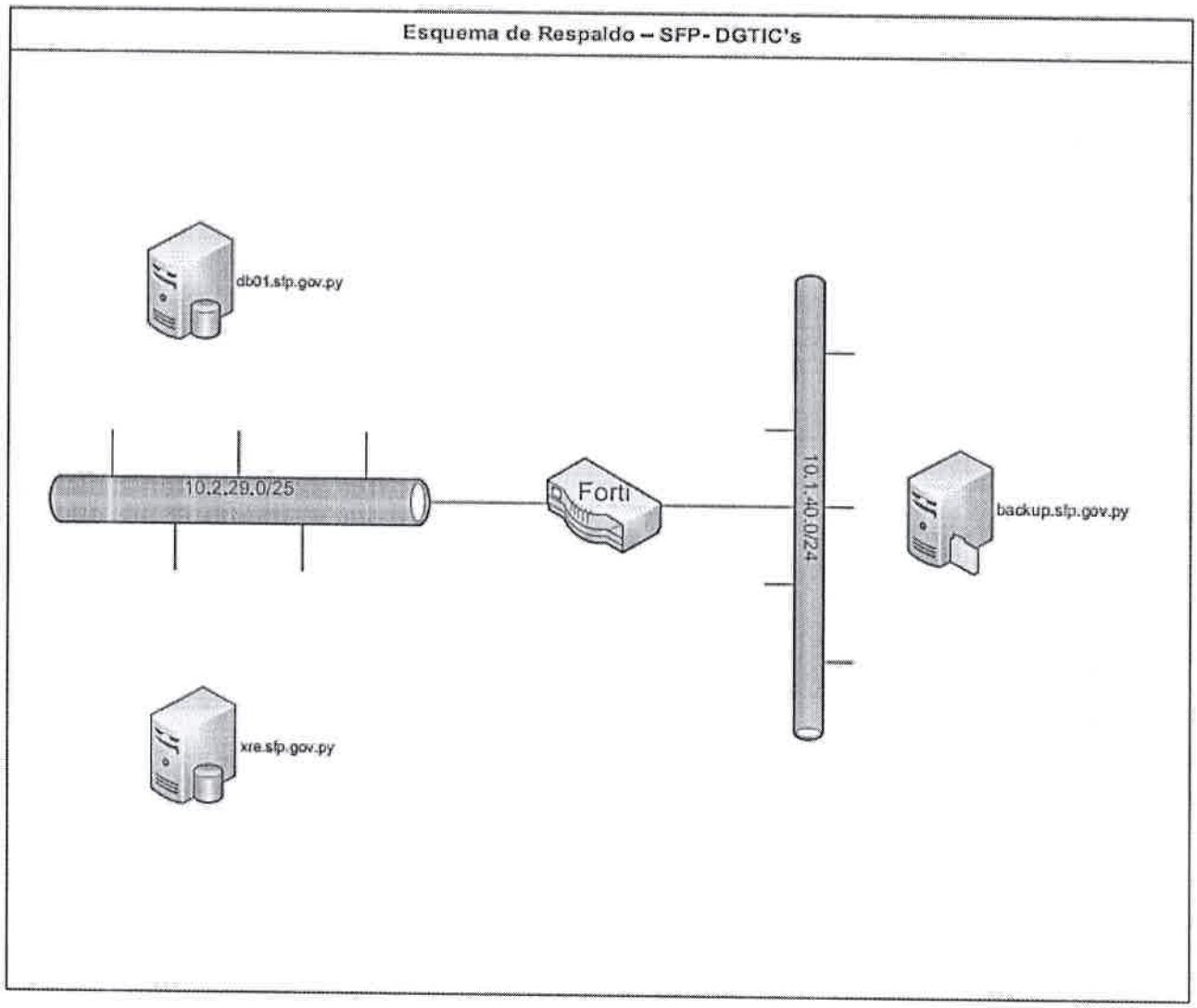
Aspectos Generales

Ejecución de tareas de backup de bases de datos de producción mediante herramientas propias de los Gerenciadores de Base de Datos (Postgresql) y trareas automáticas del demonio CROND de los Sistemas Operativos asociados.

Transferencia de archivos generados al servidor de respaldo vía autenticación por firma digital.

Elaborado por Alcides Rodriguez

Esquema de Respaldo de Datos



Activos

→ Base de Datos SICCA db01.sfp.gov.py(10.2.29.182), Sistema base Red Hat Enterprise Linux 6.7 versión de motor de base de datos (PostgreSQL) 8.4.20

→ Base de Datos XRE xre.sfp.gov.py (10.2.29.140), Sistema base CentOS release 6.7 (Final) versión de motor de base de datos 9.3.10.

→ Servidor de respaldo (backup.sfp.gov.py –10.1.40.205), Sistema base Red Hat Enterprise Linux Server release 6.2.

MINISTERIO DE ECONOMÍA Y FINANZAS
VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL
REPÚBLICA DEL PARAGUAY
Elaborado por Alcides Rodriguez A.

Procedimientos

Generación de par de claves de firma digital (Private/Public) para obtención de acceso directo al servidor de almacenamiento.

Ejecución de tareas programadas en Servidores de Bases de Datos vía demonio CROND.

Transferencia de archivos generados vía rsync.

Detalles de Procedimiento

Generar firmas digitales.

Se procede a generar una firma digital (firma digital pública) tipo DSA (Digital Signature Algorithm o Algoritmo de Firma digital) en el servidor **db01.** Se puede crear una firma tipo RSA, pero es poco recomendado debido a las puertas traseras que pudiera tener. Si se utiliza la firma digital sin contraseña, jamás se debe establecer una durante la generación de la firma digital. Cuando el diálogo solicite una contraseña con confirmación, sólo se pulsa la tecla (↵ ENTER) y se continúa el procedimiento. Si asigna contraseña, está será utilizada para autenticar el certificado creado cada vez que se quiera utilizar éste perdiendo sentido el intento de acceso directo.

ssh-keygen -t dsa

```
-bash-4.1$ hostname
db01.sfp.gov.py
-bash-4.1$ id
uid=26(postgres) gid=26(postgres) grupos=26(postgres)
-bash-4.1$ ssh-keygen -t dsa
```

Lo anterior especifica el anfitrión donde se obtiene el nombre del servidor, el usuario que realiza la petición de generación de claves de firma digital con el comando ssh-keygen de tipo dsa. Ante la petición de parámetros para la generación del par de claves, se ingresa valores por defecto(Pulsar Intro).

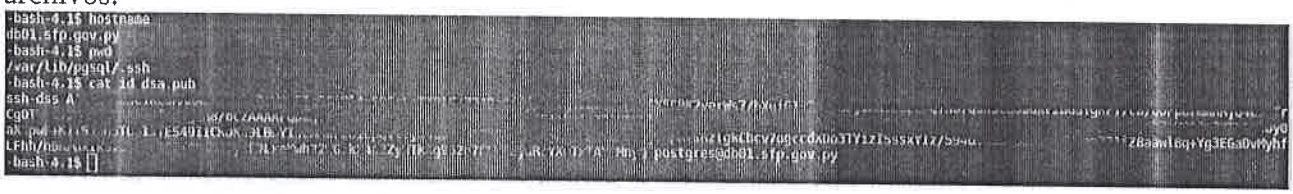
MINISTERIO DE ECONOMÍA Y FINANZAS
VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL
REPÚBLICA DEL PARAGUAY

Elaborado por Alcides Rodríguez

```
-bash-4.1$ id
uid=26(postgres) gid=26(postgres) grupos=26(postgres)
-bash-4.1$ hostname
db01.sfp.gov.py
-bash-4.1$ pwd
/var/lib/pgsql/.ssh
-bash-4.1$ ls |grep dsa
id_dsa
id_dsa.pub
-bash-4.1$
```

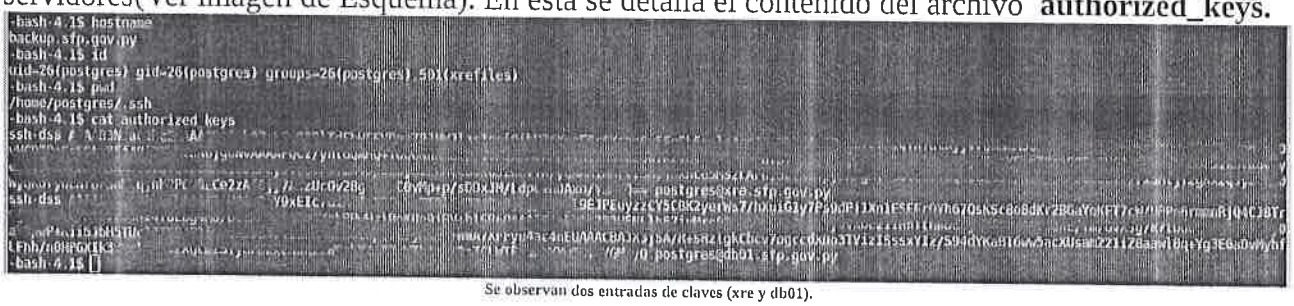
Lo anterior especifica el par de claves de firma digital privada y pública respectivamente(id_dsa, id_dsa.pub).

EL contenido de la clave pública generada(id_dsa.pub) debe ser exportada al servidor en dónde se creará la relación de confianza, específicamente debe ser agregada al fichero **~/authorized_keys** del usuario asociado al proceso a fin de poder utilizar la herramienta rsync para la transferencia de archivos.



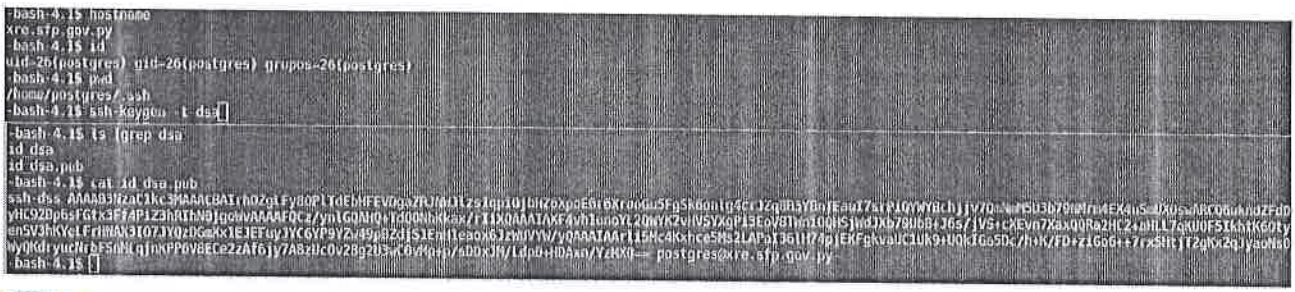
Lo anterior muestra el contenido del archivo id_dsa.pub del usuario postgres.

La siguiente imagen muestra el servidor que hace de storage de los datos generados en los otros servidores(Ver imagen de Esquema). En esta se detalla el contenido del archivo **authorized_keys.**



Se observan dos entradas de claves (xre y db01).

El mismo procedimiento debe ser realizado en el servidor **xre.**



Detalle del Demonio Crond para las tareas programadas en servidor db01.

```
-bash-4.1$ crontab -l
*/5 * * * * /var/lib/pgsql/scripts_backup/sincroniza_arcs.sh
00 23 * * * /var/lib/pgsql/scripts_backup/backup_full.sh
30 23 * * * /var/lib/pgsql/scripts_backup/sincroniza_full.sh
-bash-4.1$ cat /var/lib/pgsql/scripts_backup/sincroniza_arcs.sh
#!/bin/bash
/usr/bin/rsync -avz --remove-source-files /vol02/backup/archives/* postgres@10.1.40.205:/sicca_backup/archives/
-bash-4.1$ cat /var/lib/pgsql/scripts_backup/backup_full.sh
bk_file="sicca_full_$(date +%Y-%m-%d).dmp"
/usr/bin/pg_dump -Fc sicca >> /vol02/backup/full/$bk_file
-bash-4.1$ cat /var/lib/pgsql/scripts_backup/sincroniza_full.sh
#!/bin/bash
/usr/bin/rsync -avz --remove-source-files /vol02/backup/full/* postgres@10.1.40.205:/sicca_backup/full/
-bash-4.1$
```

Detalle de horarios y scripts de tareas programadas.

Detalle del Demonio Crond para las tareas programadas en servidor xre.

```
-bash-4.1$ crontab -l
00 23 * * * /home/postgres/scripts/bkp
30 23 * * * /home/postgres/scripts/moverbkp
-bash-4.1$ cat /home/postgres/scripts/bkp
#!/bin/bash
a="$(date +%Y-%m-%d)"

/usr/pgsql-9.3/bin/pg_dump --blobs --format=c --compress=9 --verbose --file=/home/postgres/dump/$a.xredmp xre 2> /home/postgres/log/$a.xrelog

cp /home/postgres/dump/$a.xredmp /home/xrefiles/backup

#older="$(ls /home/postgres/dump/ -c |tail -1)"
#rm /home/postgres/dump/$older

#older="$(ls /home/postgres/log/ -c |tail -1)"
#rm /home/postgres/log/$older


#older="$(ls /home/xrefiles/backup/ -c |tail -1)"
#rm /home/xrefiles/backup/$older
-bash-4.1$ cat /home/postgres/scripts/moverbkp
#!/bin/bash
/usr/bin/rsync -avz --remove-source-files /home/postgres/dump/* postgres@10.1.40.205:/xre_backup/
-bash-4.1$
```

Detalle de horarios y scripts de tareas programadas.

Fin del documento.

MINISTERIO DE ECONOMÍA Y FINANZAS

Firmado por **Juan Aguilera**,
Dir. Gral. TIC
Viceministerio de Capital Humano y Gestión Organizacional

Elaborado por Alcides Rodriguez.

DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL

INFORME FINAL A.I.I Nº 16/2023

AUDITORÍA ESPECIALIZADA Y/O INTEGRAL

AUDITORÍA INFORMÁTICA

"PLAN DE MEJORAMIENTO"

PERIODO DE REVISIÓN: AÑO 2023

FECHA DEL INFORME: DICIEMBRE 2023

MINISTERIO DE ECONOMÍA Y FINANZAS * VICEMINISTERIO DE CAPITAL HUMANO Y GESTIÓN ORGANIZACIONAL * REPÚBLICA DEL PARAGUAY

PMI

PLAN DE MEJORAMIENTO INSTITUCIONAL											
Institución:											
Máxima Autoridad:											
Auditor Interno:											
Correoelectrónico:											
Telefono:											
Informe N°			Fecha	Resolución /Orden de trabajo N°	Periodo auditado		Tipo de auditoria		Áreas de riesgo analizadas		
(1) N° Observ. s/Informe	(2) Código Hallazgo	(3) Debilidad – Hallazgo	(4) Recomendación	(5) Acción de Mejoramiento	(6) PERIODO DE EJECUCIÓN		(7) Responsable de Ejecución		(8) Indicador de Cumplimiento (Definir meta)	(9) Autoevaluación (Seguimiento del área)	
					(6.1) Fecha de Inicio	(6,2) Fecha de Finalización	(7,1) Responsable Directo	(7,2)Responsable Area		Avance de cumplimiento (%) - Comentario Fecha de revisión	

Elaborado por:	Fecha:
Revisado por:	Fecha:
Aprobado por:	Fecha: