# POLÍTICAS Y PROCEDIMIENTOS DE LOS CONTROLES GENERALES DE LOS SISTEMAS DE INFORMACIÓN

## OFICINA DE COORDINACIÓN Y DESARROLLO INSTITUCIONAL

***AUTORIZÓ:***

Licda. Sandra Edibel Guevara Pérez
**Ministra de Trabajo y Previsión Social**.

***VISTO BUENO:***

Licda. Agustina Beatriz De Paul Flores
**Directora Ejecutiva.**

***ELABORÓ:***

Ing. Juan Francisco Sánchez
**Jefe Unidad de Desarrollo Tecnológico.**

***REVISÓ:***

José Federico Bermúdez Vega
**Jefe Oficina de Coordinación y Desarrollo Institucional.**

**Ministerio de Trabajo y Previsión Social**

EL MINISTRO DE TRABAJO Y PREVISIÓN SOCIAL,

CONSIDERANDO:

**I.** Que el artículo 5 de las Normas Técnicas de Control Interno del Ministerio de Trabajo y Previsión Social, establece que es responsabilidad del nivel superior del MTPS, el diseño, aprobación e implementación de las Políticas de Control Interno.

**II.** Que el artículo 40 del mismo cuerpo normativo señala que el Nivel Superior del MTPS, a través de la Oficina de Coordinación y Desarrollo establecerá las Políticas que se establecerán en la Institución.

**III.** Que mediante memorándum de fecha 30 de los corrientes, la Oficina de Coordinación y Desarrollo Institucional, solicitó la aprobación de la Política y Procedimiento de los Controles Generales de los Sistemas de Información.

Por lo tanto, **ACUERDA:**

**I.** Aprobar en todas sus partes el documento denominado **POLÍTICAS Y PROCEDIMIENTOS DE LOS CONTROLES GENERALES DE LOS SISTEMAS DE INFORMACIÓN.** En los términos presentados por la Oficina de Coordinación y Desarrollo Institucional.

**II.** Designar a la Oficina de Coordinación y Desarrollo como responsable de la divulgación de la referida normativa. **COMUNÍQUESE.**

# POLÍTICA Y PROCEDIMIENTOS DE LOS CONTROLES GENERALES DE LOS SISTEMAS DE INFORMACIÓN

## Capítulo I
Disposiciones Generales

### OBJETIVO
**Art.1.** Establecer las políticas aplicables para la Gestión de la Regulación del uso de los recursos Informáticos y Servicios de Red.

### ALCANCE
**Art.2.** Las políticas contempladas en este normativo son aplicables a todas las áreas y dependencias del Ministerio de Trabajo y Previsión Social.

### DEFINICIONES Y MARCO CONCEPTUAL
**Art.3.** La regulación del uso de los recursos informáticos y servicios de red que la Unidad de Desarrollo Tecnológico proporciona a los empleados del Ministerio de Trabajo y Previsión Social, para su utilización en las actividades laborales diarias, estandarizar y contribuir al desarrollo informático y de sistemas.

### POLÍTICA Y DEFINICIONES TECNOLÓGICAS
**Art.4.** Se entiende por Políticas tecnológicas, al conjunto de lineamientos, directrices, reglas y procedimientos, que deben respetar todos los empleados que hacen uso de la infraestructura tecnológica existente en el Ministerio de Trabajo y Previsión Social y sus dependencias, siendo responsabilidad de los Directores, Jefes Departamentales, Jefes de Unidades, Jefes Regionales, vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

A los efectos de la presente normativa se entenderá por:

- **Institución:**
  Ministerio de Trabajo y Previsión Social.
- **Recursos y Equipo informáticos:** Todos los medios de cualquier naturaleza, físicos o lógicos que antevienen en los sistemas de

información y en las redes de comunicaciones, medio físico capaz de recibir, procesar, mostrar o almacenar datos.

- **Responsable:** Es la persona que ha de velar por el buen uso de los recursos bajo su tutela.

- **Usuario:** Es la persona que tiene alguna vinculación con la Institución y utiliza los recursos, servicios informáticos ofrecidos por la misma.

La presente regulación es aplicable a todos los miembros de la Institución, en cuanto hagan uso de recursos informáticos o servicios de red, así como a cualquier otra persona o entidad externa a la Institución que circunstancialmente los utilice.

Con objeto de dar la mayor publicidad a esta normativa, la Unidad de Desarrollo Tecnológico dispondrá de los medios necesarios para permitir su consulta de forma fácil, teniendo en cuenta que el desconocimiento de esta normativa no exime de su cumplimiento.

La utilización de los recursos informáticos y servicios de red de la Institución se ajustará a las previsiones generales del ordenamiento jurídico, especialmente en materia de protección de datos de carácter personal, propiedad intelectual e industrial y protección del honor e intimidad y, en su caso, a las propias de esta Institución.

La asistencia técnica que presta la Unidad de Desarrollo Tecnológico está exclusivamente dirigida a aquellos equipos informáticos que sean propiedad de la Institución, inventariados y se encuentren ubicados en los locales de la Institución, y aquellos equipos que los proveedores de servicios han brindado a la Institución.

## CAPITULO II

## LINEAMIENTOS PARA LA ADQUISICION DE BIENES DE INFORMATICA Y SISTEMAS.

DESARROLLO:

**Art. 5.** Toda adquisición de tecnología y de sistemas que se haga en el Ministerio de Trabajo y Previsión Social y sus dependencias deberá contar con el concepto

técnico de la Unidad de Desarrollo Tecnológico y apegarse estrictamente a la normativa que emane de la Unidad de Adquisiciones y Contrataciones Institucional.

**Art. 6.** Las operaciones relativas a la adquisición de bienes informáticos y de sistemas, establecerá prioridades y en su elección se tomará en cuenta: estudio técnico, precio, calidad, experiencia, nivel de desarrollo tecnológico, estándares y capacidad, entendiéndose por:

- Precio: costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.
- Calidad: Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
- Experiencia: presencia en el mercado nacional e internacional, estructura de la confiabilidad de los bienes y certificados de calidad con los que se cuente.
- Nivel Tecnológico: se deberá analizar el grado de obsolescencia, el nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
- Estándares: toda adquisición se basará en estándares comunes al mercado aceptados por la Unidad de Desarrollo Tecnológico.
- Capacidades: Analizar si el producto satisface la demanda actual con un amplio margen y si tiene capacidad de crecimiento para soportar la carga de trabajo del área en la cual será implementado.

**Art. 7.** Para la adquisición de hardware se observará lo siguiente:

- Los equipos que se adquieran, deberán estar dentro de los productos vigentes de los fabricantes y dentro de los estándares del Ministerio de Trabajo y Previsión Social.
- Deberán ser cubiertos por una garantía que se especifique claramente y por escrito en los documentos de compra (facturas, recibos, créditos fiscales, etc.).
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional o bien internacional, así como con asistencia técnica local.

- Los equipos, impresoras, scanner integrados, plotters, cámaras, etc., deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en el Ministerio de Trabajo y Previsión Social, corroborando que los suministros *(cintas, papel, toner, cartuchos etc.)* se adquieran fácilmente en el mercado y no estén sujetas a un solo proveedor.

- Los equipos adquiridos deberán contar con asistencia técnica por parte del proveedor durante la instalación de los mismos, salvo disposiciones especiales determinadas al momento de la compra.

**Art. 8.** En cuanto se refiere a los computadores personales y los servidores, equipos de comunicaciones como enrutadores y concentradores de medios, y otros que se justifiquen por ser de operación crítica o bien de alto costo; al vencer su período de garantía, deben contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos.

**Art. 9.** En la adquisición de equipos de cómputo, se deberá incluir el software de sistema operativo vigente precargado con su licencia correspondiente, para el efecto se tendrán en cuenta los lineamientos para la adquisición de software que se enuncia en este documento.

**Art. 10.** La Unidad de Activo Fijo deberá mantener un inventario actualizado de los equipos informáticos adquiridos por el Ministerio de Trabajo y Previsión Social y se mantendrá control de los mismos bajo los lineamientos de dicha Unidad.

## CAPITULO III

## INSTALACIÓN

**Art. 11.** Los equipos de la entidad se instalarán en lugares adecuados, lejos de polvo y en la medida de los posible del tráfico de personas y garantizando las condiciones para su adecuado funcionamiento.

**Art. 12.** Las instalaciones eléctricas y de comunicaciones, deberán cumplir con los estándares vigentes y resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.

**Art. 13.** En ningún caso, se permitirán instalaciones improvisadas o sobre cargadas.

## CAPITULO IV

## FUNCIONAMIENTO

**Art. 14.** Los empleados del Ministerio de Trabajo y Previsión Social y sus dependencias al usar los equipos de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o puedan deteriorar la información almacenada en medios magnéticos.

**Art. 15.** El usuario no instalará ningún tipo de software (estandarizado o no, shareware, freeware, demo, de dominio público, etc.) en los equipos sin la aprobación expresa de la Unidad de Desarrollo Tecnológico (dicha aprobación se solicitará y concederá por escrito).

**Art. 16.** Los funcionarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos del Ministerio de Trabajo y Previsión Social y sus dependencias mediante la utilización de contraseñas confidenciales.

**Art. 17.** Todas las acciones realizadas bajo los auspicios de un identificador de usuario (Nombre de Usuario y contraseña de acceso) y sus consecuencias legales son responsabilidad del usuario titular del identificador.

**Art. 18.** Cada usuario es responsable del cuidado del hardware y software suministrado por la entidad. En consecuencia cada usuario responderá solidariamente por los daños y perjuicios técnicos y/o legales ocasionados por su mala utilización (La detección de este uso indebido podrá ocasionar la inhabilitación temporal o definitiva del sistema para el usuario responsable).

**Art. 19.** La Unidad de Desarrollo Tecnológico, es la dependencia responsable de coordinar con la Unidad de Activo Fijo y la Unidad de Adquisiciones y Contrataciones Institucionales, la reparación de los equipos de cómputo de propiedad del Ministerio de Trabajo y Previsión Social. Las reparaciones y/o ampliaciones de los equipos no pueden ser hechas o contratadas por el usuario.

**Art. 20** Todo el hardware conectado a la red debe ser autorizado por la Unidad de Desarrollo Tecnológico, no pueden conectarse computadoras desautorizadas, servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

## CAPITULO V

## *SEGURIDAD*

**Art. 21.** Para la seguridad de los recursos informáticos del Ministerio de Trabajo y Previsión Social, la Unidad de Desarrollo Tecnológico debe promover el establecimiento de seguridades físicas y lógicas, para lo cual se estable lo siguiente:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado (Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios, deben expirar periódicamente y poseer una longitud mínima).

- Verificar la información que provenga de fuentes externas, a fin de corroborar que estén libres de cualquier agente externo que pueda contaminarla o perjudique el funcionamiento de los equipos.

- Mantener pólizas de seguros de los recursos informáticos en funcionamiento (Se debe incluir en la póliza colectiva de seguros el riesgo ante posibles pérdidas de información, por daños irrecuperables en los medios de almacenamiento).

- Los empleados adscritos a la Unidad de Desarrollo Tecnológico deberán suscribir un acuerdo de confidencialidad que estará vigente durante y después de haber ocupado un cargo dentro de la Unidad de Desarrollo Tecnológico.

## CAPITULO VI

## SEGURIDAD FISICA

**Art. 22.** El área de la Unidad de Desarrollo Tecnológico del Ministerio de Trabajo y Previsión Social *(Cuartos de equipos de cómputo, Cuartos de UPS, etc.)* deberá tener acceso restringido a personas no autorizadas.

**Art. 23.** Todos los empleados autorizados por la Unidad de Desarrollo Tecnológico, deberán portar el carnet en lugar visible, permitiendo con esto una mejor identificación y control de las personas que ingresan a las áreas de cómputo restringidas.

**Art. 24.** Los bienes informáticos serán cargados al inventario del funcionario responsable y su movilización no se podrá realizar sin la aprobación de la Unidad de Activo Fijo y la Unidad de Desarrollo Tecnológico, quienes son las encargadas de administrar los bienes informáticos.

**Art. 25.** Solo personal técnico autorizado por el Jefe de la Unidad de Desarrollo Tecnológico puede revisar, configurar y dar soporte a los bienes informáticos del Ministerio de Trabajo y Previsión Social.

## CAPITULO VII

## SEGURIDAD LOGICA

**Art. 26.** Los usuarios tienen la obligación de cambiar periódicamente su clave de acceso, de acuerdo a los lineamientos establecidos por la Unidad de Desarrollo Tecnológico.

**Art. 27.** Todas las aplicaciones que se utilicen deben tener clave de acceso y establecer perfiles de usuario para acceder a la información.

**Art. 28.** Las palabras claves no deben aparecer en la pantalla al ser ingresadas, tampoco deben imprimirse o mantenerse en la máquina, ni en un medio que se encuentre en lugar visible.

**Art. 29.** El administrador de la red y el administrador de la base de datos cambiarán inmediatamente las claves de acceso a los empleados o contratistas que tengan ausencias definitivas de sus cargos o terminación de sus contratos.

**Art. 30.** Cuando un usuario maneje aplicaciones específicas y sea removido de su puesto de trabajo de manera provisional o permanente, deberá hacer entrega formal del equipo a su cargo, las claves de acceso e instruir a su remplazó en la utilización del software que administra.

**Art. 31.** Todo medio de almacenamiento (CD, cinta, unidad USB, etc.) que ingrese a la Entidad deberá ser previamente revisado en búsqueda de virus, spyware o software malintencionado.

## CAPITULO VIII

## USO PROHIBIDOS

**Art. 32.** Se considerará el abuso en la utilización de recursos informáticos como una falta disciplinaria. En el entendido que el presente documento de políticas es solo un marco de referencia para los usuarios y en virtud de la imposibilidad de enumerar toda prohibición existente, se deja constancia de que todo aquello que no se encuentra expresamente permitido se encuentra restringido.

**Art. 33.** Queda prohibida la utilización de cualquier recurso informático del Ministerio de Trabajo y Previsión Social de manera que viole cualquier ley nacional o internacional.

**Art. 34.** Queda prohibida la utilización de cualquier recurso informático de la Red para almacenar o portar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de

actividades lucrativas en general, o su utilización en actividades no relacionada con las funciones propias del cargo.

**Art. 35.** Queda prohibida la instalación de hardware y/o software sin la autorización apropiada de la Unidad de Desarrollo Tecnológico

**Art. 36.** No permitir a personal externo acceder información de la Red sin la autorización de la Unidad de Desarrollo Tecnológico.

**Art. 37.** Queda prohibida la utilización de identificadores (Nombre y Password) de usuarios ajenos.

**Art. 38.** Queda prohibida la creación, utilización o distribución de programas que puedan dañar los datos, archivos, aplicaciones, funcionamientos del sistema, o funcionamientos de la red.

**Art. 39.** Queda prohibid el capturar o intentar desencriptar contraseñas y/o protocolos de comunicaciones.

**Art. 40.** Queda prohibida la utilización de la Red para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.

**Art. 41.** Queda prohibida la utilización de cualquier software o hardware que pueda comprometer la seguridad de la red y/o de cualquier recurso informático de la

misma.

**Art. 42.** Queda prohibido el acceso a cualquier espacio virtual restringido para el que no se dispone de la debida autorización.

**Art. 43.** Queda prohibida la introducción intencionada de virus, "caballos de Troya", "gusanos", "bombas de tiempo" o cualquier otro software perjudicial o nocivo.

**Art. 44.** Queda prohibido el saboteo del uso de la red mediante la congestión de enlaces o sistemas informáticos, interceptación de las comunicaciones y la utilización de técnicas de escucha, transmisión, grabación o reproducción de cualquier señal de comunicaciones.

**Art. 45.** Queda prohibido el acceso a Internet con fines comerciales o recreativos (Chat, descarga de archivos Mp3 u otros).

**Art. 46.** Queda prohibida la afectación del ancho de banda con la descarga de archivos grandes de música, imágenes, videos, emisoras de radio y de TV., etc.

## CAPITULO IX

## POLÍTICA SOBRE OBSOLESCENCIA.

**Art. 47.** Se considera un equipo de cómputo obsoleto, cuando el costo anual por mantenerlo en operación sea igual o superior al 50% del costo del bien de nueva adquisición que lo sustituiría, asimismo, cuando se haya agotado toda posibilidad de que pueda ser utilizado como herramienta de apoyo eficaz para atender los requerimientos de procedimiento de información de la dependencia o entidad.

**Art. 48.** El titular de la Unidad de Desarrollo Tecnológico deberá hacer constar que no es posible instalar software que resuelva eficientemente las necesidades actuales en dicho equipo de cómputo que lo incorpore a las actividades de la dependencia.

**Art. 49.** Esta permitido extraer los componentes físicos de un equipo de cómputo que se considere obsoleto para incluirlos en otro equipo de cómputo a efecto de subsanar la obsolescencia del segundo y asegurar mayor tiempo de vida útil. El titular de la Unidad de Desarrollo Tecnológico será el responsable de llevar un registro y control de dichas trasferencias, asimismo, de la justificación correspondiente.

**Art. 50.** Los equipos que se consideren obsoletos implicarán la baja de los mismos del inventario de la dependencia o entidad una vez la comisión evaluadora así lo haya determinado a sugerencia del titular de la Unidad de Desarrollo Tecnológico.

**Art. 51.** Los cambios en el inventario de equipo de cómputo de la dependencia o entidad derivados de la obsolescencia de los mismos, deberá llevarse en el correspondiente control de la Unidad de Activo Fijo.

**Art. 52.** APLICACIÓN DE LA POLÍTICA: La aplicación de la presente política para la compra de bienes por sustitución, será dependiente de la disponibilidad económica en el rubro correspondiente de la dependencia o del Ministerio.

## CAPITULO X

## POLÍTICA DE CONTROL DE ACCESOS.

**Art. 53.** En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
d) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

**Art. 54. Reglas de Control de Acceso**

Las reglas de control de acceso especificadas, establecen:

a) Todas las reglas son obligatorias.
b) Todo debe estar prohibido a menos que se permita expresamente.
c) Controlar las reglas que requieren la aprobación de los administradores de sistemas, antes de entrar en vigencia, y aquellas que no requieren aprobación.

**Art. 55. Administración de Accesos de Usuarios**

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

**Art. 56. Administración de Usuarios**

Se definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
b) Solamente el Propietario de la Información podrá hacer solicitudes y revocación de acceso a los sistemas que procesan su información.

c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Control de Accesos del Ministerio de Trabajo y Previsión Social.

d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.

e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

f) Mantener un registro formal de todas las personas registradas para utilizar el servicio.

g) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Ministerio de Trabajo y Previsión Social o sufrieron la pérdida/robo de sus credenciales de acceso.

h) Efectuar revisiones periódicas con el objeto de:
   - cancelar identificadores y cuentas de usuario redundantes
   - inhabilitar cuentas inactivas por más de 60 días
   - eliminar cuentas inactivas por más de 120 días

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.

l) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

**Art. 57 Administración de Privilegios**

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.

Mantener un proceso de autorización y un registro de todos los privilegios asignados.

Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación.

**Art. 58. Administración de Contraseñas de Usuario**

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto.
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Configurar los sistemas de tal manera que:
   - Las contraseñas tengan no menos de 8 caracteres.
   - Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta.
   - solicitar el cambio de la contraseña cada 30 días.
   - impedir que las últimas 12 contraseñas sean reutilizadas.
   - establecer un tiempo de vida mínimo no mayor a 3 días para las contraseñas.

**Art. 59. Administración de Contraseñas Críticas**

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como la instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el usual. Se definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
b) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
c) La utilización de las contraseñas críticas será registradas, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen.
d) con la misma.
e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas.

**Art. 60. Revisión de Derechos de Acceso de Usuarios**

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de 6 meses, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de 6 meses.
b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses.
c) Revisar las asignaciones de privilegios a intervalos de 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

**Art. 61. Responsabilidades del Usuario**

**Uso de Contraseñas**

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso los servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
- Sean fáciles de recordar.
- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión.
g) Notificar cualquier incidente de seguridad relacionado con sus contraseñas pérdida, robo o indicio de pérdida de confidencialidad.

**Art. 62. Equipos Desatendidos en Áreas de Usuarios**

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo,

requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

Proteger las Computadoras o terminales contra usos no autorizados mediante un bloqueo de sesión.

**Art. 63. Seguridad de los Servicios de Red**

Se definirán pautas para garantizar la seguridad de los servicios de red del Ministerio de Trabajo y Previsión Social, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

a) Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
b) Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
c) Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
d) Instalar periódicamente las actualizaciones de seguridad.

**Art. 64. Identificación y Autenticación de los Usuarios**

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.
b) Registrar los poseedores de autenticadores.
c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

## CAPITULO XI

## POLÍTICA DE ADMINISTRACIÓN DE CENTROS DE DATOS.

### Art. 65. Instalación de Sistema Operativo

Es responsabilidad del administrador de servidores la instalación del Sistema Operativo para los equipos mencionados por lo que debe de asegurarse de la correcta instalación y seguridad por medio firewall de software.

Otras actividades:

a) Crear nuevos usuarios.
b) La restauración de contraseñas de usuario.
c) Bloqueo / desbloqueo de cuentas de usuario.
d) Monitor de la seguridad del servidor.
e) Monitor de servicios especiales.
f) Administración de usuarios (instalación y mantenimiento de cuentas).

g) El mantenimiento de sistema.
h) Comprobar que los periféricos funcionan correctamente.
i) En caso de fallo de hardware, el designa los horarios de reparación.
j) Monitor de rendimiento del sistema.
k) Estables y validar la proceso de copias de seguridad y recuperación de los servicios especiales.
l) Monitor de la comunicación de red.
m) Actualizar los sistemas según sean accesibles nuevas versiones de SO.
n) Aplicar las políticas para el uso del sistema informático y de red.

### Art. 66. Control de Servicio

La responsabilidad del administrador de Servidores de llevar una controles de servicio por cada equipo haciendo una lista de los puertos de acceso y no de los servicio debido a que es responsabilidad de que administra el servicio de darle la seguridad debida adicional.

### Art. 67. Control de Acceso

La responsabilidad del administrador de asignar el acceso físico a los técnicos y de llevar una bitácora de acceso al Data Center. También de definir los acceso a los servicios red o a los equipos asimismo de un control de usuario y clave para ingresar

a dichos equipos. Este proceso sería mucho más factible si se contara con un control biométrico (Anexo Control de Acceso a Sala de Servidores).

**Art. 68. Monitoreo de los Servicios Especiales**

Es responsabilidad del Administrador de Servidores monitorear los diferentes servicios especiales (entenderemos como servicios especiales aplicación Web, Base de Datos y de conectividad a los servicio especial) y exigir al administrador del servicio especial un reporte de actividades realizada a fin de que el servicio cumpla su buen funcionamiento.

**Art. 69. Control del Ambiente**

Es responsabilidad del administrador de servidores que el ambiente donde se encuentra alojado los servidores cumpla con los estándares mínimos requerido y de verificar el buen funcionamiento de los aires acondicionado y eléctricos.

**Art. 70. Garantías**

El responsabilidad del Administrador de Servidores tramitar las garantías por falla física y de llevar un control de las garantías de cada equipo del Data Center.

## CAPITULO XII

## CICLO DE VIDA DE LOS SISTEMAS INFORMÁTICOS

**Art. 71. El ciclo de vida de los proyectos de desarrollo de sistemas informáticos considera 7 fases, estas se deberán registrar en formato digital y físico bajo la siguiente estructura:**

1. Planificación
2. Análisis
3. Diseño
4. Desarrollo
5. Pruebas
6. Implementación
7. Cierre

Los entregables que se deberán generar en cada fase del ciclo de vida de los proyectos de desarrollo de sistemas informáticos son los siguientes:

1. Planificación
   1.1. Solicitud de sistema / Anteproyecto
   1.2. Acta de constitución del proyecto

2. Análisis
   2.1. Recolección y análisis de requerimientos
   2.2. Análisis FODA
   2.3. Definición de Estructura Desglosada de Trabajo (EDT)
   2.4. Cronograma de actividades del proyecto
3. Diseño
   3.1. Prototipo del sistema
   3.2. Acta de aceptación de prototipo del sistema

4. Desarrollo
   4.1. Definición de la lista de tareas (Product backlog)
   4.2. Definición de iteraciones (Sprint)
      4.1.1. Desarrollo
      4.1.2. Demostración
      4.1.3. Pruebas unitarias
      4.1.4. Solicitudes de cambio
   4.3. Acta de aceptación de desarrollo del sistema

5. Pruebas
   5.1. Guía de pruebas de integración
   5.2. Resultado de pruebas de integración
   5.3. Acta de aceptación de pruebas del sistema

6. Implementación
   6.1. Acta de implementación del sistema
   6.2. Manual de uso

7. Cierre
   7.1. Informe de cierre del proyecto

*Las minutas de reunión se generarán en cada etapa según sea necesario.

**Art. 72. Desarrollo de los sistemas informáticos**

Toda solicitud para nuevos sistemas informáticos deberá ser presentada por escrito por la jefatura de la oficina usuaria a la jefatura de la Unidad de Desarrollo Tecnológico.

La jefatura de la Unidad de Desarrollo Tecnológico analizará la solicitud del nuevo sistema informático junto al personal del Área de Desarrollo de Sistemas, luego autorizará el inicio del nuevo proyecto de desarrollo del sistema informático solicitado.

La persona responsable del Área de Desarrollo de Sistemas tomará el rol de persona administradora del proyecto y convocará a reunión a la jefatura de la oficina usuaria y a una persona responsable del proceso de dicha oficina, para dar a conocer las etapas del nuevo proyecto de desarrollo del sistema informático y establecer las necesidades de manera general, con base en lo anterior se deberá generar el "Acta de constitución del proyecto".

La jefatura de la oficina usuaria presentará por escrito los requerimientos del nuevo sistema informático a la jefatura de la Unidad de Desarrollo Tecnológico y al Área de Desarrollo de Sistemas.

La persona administradora del proyecto con base a los requerimientos recibidos, realizará un análisis FODA (Debilidades / Fortalezas / Amenazas / Oportunidades) sobre el nuevo proyecto de desarrollo del sistema informático.

La persona administradora del proyecto junto con equipo de trabajo desglosarán las tareas de acuerdo al esfuerzo a realizar en cada etapa, de esta manera definirán entregables que generen valor agregado al producto final.

Luego del establecimiento de tareas, sigue la asignación de tiempo para realizar cada una de ellas, será la persona administradora del proyecto junto al equipo de trabajo quienes definan un cronograma de actividades del nuevo proyecto de desarrollo del sistema informático y posteriormente realizarán una presentación a la jefatura de la oficina usuaria y a la persona responsable del proceso de dicha oficina.

El equipo de trabajo creará un prototipo del nuevo sistema informático, este implicará el diseño de pantallas de entrada y salida de datos, reportes, gráficos, entre otros. En una reunión de seguimiento, la persona administradora del proyecto junto al equipo de trabajo presentarán el diseño del nuevo sistema a la jefatura de la oficina usuaria y a la persona responsable del proceso de dicha oficina, quienes podrán realizar observaciones respecto del diseño propuesto.

De existir cambios en el diseño del nuevo sistema informático, los realizará el equipo de trabajo y serán presentados en una reunión de seguimiento a la jefatura de la oficina usuaria y a la persona responsable del proceso de dicha oficina, se espera obtener la aprobación final y plasmarla en el "Acta de aceptación de prototipo del sistema"

El desarrollo de los sistemas informáticos se llevará a cabo mediante la adopción de la metodología ágil SCRUM, esto implicará que la persona administradora del proyecto junto a la persona responsable del proceso de la oficina usuaria definan la lista de tareas (Product backlog) a realizar por el equipo de trabajo en cada iteración (Sprint), la iteración puede durar un periodo de 5 a 20 días, esto varía según la complejidad de los requerimientos. Cada iteración comprende: Desarrollo, demostración, pruebas unitarias y solicitudes de cambio; al finalizar cada iteración se realizará una retroalimentación donde participarán la persona administradora del proyecto y la persona responsable del proceso de la oficina usuaria, así mismo, se realizarán reuniones de planificación (Sprint planning) para las siguientes iteraciones que requiera el nuevo proyecto de desarrollo del sistema informático.

Al finalizar las iteraciones requeridas para el nuevo proyecto de desarrollo del sistema informático y obtener el producto final, el cual será aprobado por la jefatura de la oficina usuaria y a la persona responsable del proceso de dicha oficina, se deberá generar el "Acta de aceptación de desarrollo del sistema".

La persona administradora del proyecto proveerá a las personas usuarias del nuevo sistema informático una guía de pruebas, que deberán seguir paso a paso e informar si se presenta algún inconveniente que les obstaculice o les impida continuar con el proceso. Al finalizar las pruebas al nuevo sistema informático se deberá generar el "Acta de aprobación de pruebas del sistema".

Las personas administradoras de la red de datos y servidores serán la responsable de presentar el ambiente de producción con los requerimientos mínimos necesarios para la instalación del nuevo sistema informático.

Las personas administradoras de la red de datos y servidores junto con el equipo de trabajo serán los encargados de instalar la versión final y aprobada del nuevo sistema informático, así mismo, deberán instalar su base de datos y cualquier otro elemento que sea requerido para el funcionamiento óptimo del servicio.

Posterior a la implementación del nuevo sistema informático, las personas administradoras de la red de datos y servidores junto con el equipo de trabajo deberán verificar que el sistema funcione adecuadamente, este proceso permitirá generar el "Acta de implementación del sistema".

La persona administradora del proyecto proveerá a las personas usuarias del nuevo sistema informático un manual de uso, que servirá de guía para realizar el proceso dentro del sistema.
Finalmente, la persona administradora del proyecto deberá generar un "Informe de cierre del proyecto", del cual debe presentar copia a la jefatura de la oficina usuaria.

**Art. 73. Mantenimiento de los sistemas informáticos**

Toda solicitud de mejoras o cambios en los sistemas informáticos deberá ser presentada por escrito por la jefatura de la oficina usuaria a la jefatura de la Unidad de Desarrollo Tecnológico.

La persona responsable del Área de Desarrollo de Sistemas tomará el rol de persona administradora del proyecto, analizará la solicitud de mejoras o cambios en el sistema informático junto al equipo de trabajo.

La persona administradora del proyecto convocará a reunión a la jefatura de la oficina usuaria y a una persona responsable del proceso de dicha oficina, para establecer las necesidades de manera general y el procedimiento de realización de mejoras o cambios en el sistema informático.

La jefatura de la oficina usuaria presentará por escrito los nuevos requerimientos del sistema informático a la jefatura de la Unidad de Desarrollo Tecnológico y al Área de Desarrollo de Sistemas.

La persona administradora del proyecto junto con equipo de trabajo desglosará las tareas de acuerdo al esfuerzo que se requiera, definirán el o los entregables y finalmente elaborarán un cronograma de actividades de mejoras o cambios en el sistema informático.

La persona administradora del proyecto junto con equipo de trabajo analizará y diseñaran las mejoras o los cambios en el sistema informático. En una reunión de seguimiento, la persona administradora del proyecto junto al equipo de trabajo presentará un prototipo a la persona responsable del proceso de dicha oficina, quien podrá realizar observaciones respecto de lo propuesto, el equipo de trabajo deberá solventar lo observado.

Posteriormente, la persona administradora del proyecto junto a la persona responsable del proceso de la oficina usuaria definan la lista de tareas (Product backlog) a realizar por el equipo de trabajo en cada iteración (Sprint). Cada iteración comprende: Desarrollo, demostración, pruebas unitarias y solicitudes de cambio; al finalizar cada iteración se realizará una retroalimentación donde participarán la persona administradora del proyecto y la persona responsable del proceso de la oficina usuaria, así mismo, se realizarán reuniones de planificación (Sprint planning) para las siguientes iteraciones si lo requiere el desarrollo de mejoras y cambios en el sistema informático.

Las personas administradoras de la red de datos y servidores junto con el equipo de trabajo deberán instalar la versión final y aprobada de las mejoras y cambios en el sistema informático, así mismo, deberán instalar su base de datos y cualquier otro elemento que sea requerido para el funcionamiento óptimo del servicio.

Posterior a la implementación de las mejoras y cambios en el sistema informático, las personas administradoras de la red de datos y servidores junto con el equipo de trabajo deberán verificar que el sistema funcione adecuadamente.

Finalmente, la persona administradora del proyecto deberá generar un informe de cierre del desarrollo de las mejoras o los cambios en el sistema informático y se deberá presentar copia a la jefatura de la oficina usuaria.

## Diseño

**Art. 74.** La Oficina de Coordinación y Desarrollo Institucional, es la responsable de diseñar el formato de cada documento institucional, con los requerimientos técnicos y legales para cada caso concreto y de acuerdo a los requerimientos de las Direcciones o Unidades del Ministerio de Trabajo y Previsión Social.

**Art. 75.** La presente Política entrará en vigencia a partir de su autorización mediante Acuerdo Ministerial y será divulgada por medio del programa GPO (Group Policy Object) a todo el Ministerio de Trabajo y Previsión Social y al través de la INTRANET.

ANEXOS

## CONTROL DE ACCESO A SALA DE SERVIDORES

| NOMBRE DE LA PERSONA | EMPRESA O INSTITUCION | FECHA DE INGRESO | HORA DE INGRESO | TRABAJO REALIZADO | FECHA DE SALIDA | FIRMA |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |