MANUAL DE INFORMÁTICA, TECNOLOGÍA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Elaboró: Sonia Yolima Guerrero **Cargo:** Asistente de Procesos **Fecha:** Octubre 2018	**Revisó:** Luz Mery Quiroz **Cargo:** Profesional de Planeación (Coordinador de Calidad) **Fecha:** Octubre 2018 **Revisó:** Darwin Narvaez **Cargo:** Director Nacional de Informática y Tecnología **Fecha:** Octubre 2018	**Aprobó:** Nubia Oyuela **Cargo:** Vicepresidente de Soporte Corporativo **Fecha:** Octubre 2018

	MANUAL DE INFORMÁTICA, TECNOLOGÍA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	**VERSIÓN: 4**
		CODIGO: MN-IT-019
		ACTUALIZACIÓN: Octubre/ 2018
		EMISIÓN: Enero/ 2016

Contenido

INTRODUCCIÓN 5

OBJETIVO 6

1. POLÍTICA DE CLASIFICACIÓN Y CONTROL DE ACTIVOS INFORMÁTICOS 6

1.1. Inventario de activos 6

1.2. Clasificación de la información 7

1.3. Rotulado de la Información 8

2. POLÍTICA DE SEGURIDAD DEL PERSONAL 9

2.1. Seguridad en la Definición de Roles y la Asignación de Recursos 9

2.1.1. Incorporación de la Seguridad en los Roles del Personal de 4-72. 9

2.2. Capacitación del Usuario 9

2.2.1. Formación y Capacitación en Materia de Seguridad de la Información 9

3. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL 10

3.1. Seguridad para Equipos de Computo 10

3.2. Mantenimiento de Equipos 11

3.2.1. Dar de Baja y/o Borrado Seguro de los Equipos 12

3.2.2. Políticas de Escritorios y Pantallas Limpias 12

4. POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIÓNES 14

4.1. Protección contra Software Malicioso 14

4.2. Backups 16

4.2.1. Residencia y Manejo de datos 16

4.2.2. Tipos de Backups: 16

4.2.3. Periodicidad y Custodia del Backup de Sistemas de Información 17

4.2.4. Retención 17

4.2.5. Datos Críticos para Ejecución de Backups 17

4.2.6. Auditoria del Proceso de Backup 18

4.2.7 Backups en Equipos de Computo 18
4.3. Administración de los Recursos de Red 19
4.4. Intercambios de Información y Software 19
4.4.1. Políticas de Seguridad de Correo Electrónico 19
4.4.2. Políticas de Adquisición de Software 20
4.4.3. Políticas de la Instalación de Software 21
5. POLÍTICA DE CONTROL DE ACCESO 22
5.1. ADMINISTRACIÓN DE USUARIOS 22
5.1.1. Creación 22
5.1.2. Deshabilitación y/o Eliminación 24
5.1.3. Modificación 24
5.1.4. Pasos para la Administración de Cuentas de Usuario 25
5.1.5. Pasos para la Inactivacion de Cuentas de Usuario 26
5.1.6. Depuración de Usuarios 28
5.1.7. Definición de Roles 28
5.2. ADMINISTRACIÓN SISTEMAS DE INFORMACIÓN Y BASE DE DATOS 29
5.2.1. Alcance de la Administración 29
5.2.2. Servicios Cubiertos en la Administración 29
5.2.3. Controles 31
5.3. Administración de Usuarios y Contraseñas 32
5.4. Control de Acceso a los Sistemas de Información 33
5.4.1. Acciones para Construir Contraseñas Seguras: 33
5.4.2. Usuarios sistemas de información 34
5.4.3. Acciones que deben evitarse en la gestión de contraseñas seguras 35
5.5. Custodia de Contraseñas de Perfil de Alto Privilegio 36
5.6. Horario de Uso de las Credenciales 36
5.7. Logs de Auditorias 37
5.7.1. Administración de los Logs de Auditorias y sus responsables. 37
6. POLÍTICAS DE UTILIZACIÓN DE CONTROLES CRIPTOGRÁFICOS 38

6.1. Uso de los controles criptográficos 38
6.2. Cifrado Unidireccional 38
6.3. Gestión de claves 39
7. **POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** 41
7.1. Notificación de incidentes de seguridad de la información 41
7.2. CONTROL DE CAMBIOS DE LOS SISTEMAS DE INFORMACIÓN 42
7.2.1. Tipos de Cambios 42
7.2.2. Roles y Responsabilidades 43
7.2.3. Integrantes sobre la Gestión del Control de Cambios y Publicaciones 44
7.2.4. Pasos para el Control de Cambios en los Sistemas de Información 45
7.3. GESTIÓN DE PROYECTOS 45
7.3.1. Metodología Aplicada 46
7.3.2. Entregables de Proyectos 46
7.4. PASO A PRODUCCIÓN DE SISTEMAS DE INFORMACIÓN 46
7.4.1. Ambientes de un Sistema de Información 46
7.4.2. Entrega de Proyectos de Sistemas de Información 47
7.5. CONTROL DE UTILIZACIÓN DE SOFTWARE Y HARDWARE 48
7.5.1. Disposición final de software y hardware 49
7.6. DOCUMENTACIÓN DE APLICACIONES 49
8. CUMPLIMIENTO DE LA POLÍTICA 49
8.1. Cumplimiento de la Política de Seguridad 49
8.2. Sanciones por Incumplimiento de la Política 49
9. IDENTIFICACIÓN DE CAMBIOS ..... **¡Error! Marcador no definido.**
5.7. Logs de Auditorias 52
5.7.1. Administración de los Logs de Auditorias y sus responsables. 52

INTRODUCCIÓN

Hoy en día los requerimientos de seguridad que involucran las tecnologías de la información han cobrado gran auge en pocos años y más aun con la aparición del internet, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situaciones que han llevado la aparición de nuevas amenazas en los sistemas computarizados, esto hace que se desarrollen políticas de seguridad que norman el uso adecuado de estas destrezas tecnológicas dando recomendaciones para aprovechar estas ventajas y evitar su uso indebido.

De esta manera la política de seguridad de la información de 4-72, emerge como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan IT cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la entidad, conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte de la alta Gerencia, con el objeto que las normas y procedimientos tienen la finalidad de definir, especificar y elaborar los requisitos y procedimientos de seguridad para la gestión de la protección de los activos de la información de la empresa, de una manera consistente y efectiva dentro del marco de la seguridad de los sistemas informáticos que son los siguientes:

- Garantizar: confidencialidad, privacidad, integridad y disponibilidad.
- Cumplir con las legislaciones y reglamentación vigente.
- Proteger los activos de información de 4-72.

OBJETIVO

Establecer las políticas en seguridad de la información de Servicios Postales Nacionales S.A., con el fin de regular la gestión de la seguridad de la información de la entidad.

1. POLÍTICA DE CLASIFICACIÓN Y CONTROL DE ACTIVOS INFORMÁTICOS

La información es identificada como un activo esencial para el desarrollado de las actividades de la entidad y debe ser resguardada bajo los principios fundamentales de confidencialidad, integridad y disponibilidad.

1.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos responsables y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad 6 meses.

Es responsabilidad del área de Almacén elaborar el inventario de activos fijos tecnológicos y actualizarlo.

Entre los tipos de activos que se pueden encontrar dentro de Servicios Postales Nacionales S.A, se incluye:

a) Información:
   - Bases de datos y archivos
   - Contratos y acuerdos
   - Documentación del sistema
   - Manuales de usuario
   - Material de capacitaciones.
   - Procedimientos operacionales o de soporte
   - Información de auditorías internas de IT
   - Información archivada

b) Activos de software:
   - Aplicaciones de software
   - Software de sistemas Licencias

- Herramientas de desarrollo y utilidades

c) Activos físicos:
- Equipos de Computo
- Equipos de comunicaciones
- Medios móviles y otros equipos (Impresoras, escáner, telefonía, lectores)

Nota: *En el numeral C, el inventario de los equipos tecnológicos (Activos Fijos) de la compañía, es responsabilidad del área de Infraestructura- Almacén, los activos físicos en arrendo en el caso de existir esta figura es responsabilidad de realizar el inventario junto con el proveedor existente, y así mismo el área de IT es responsable de suministrar dichos elementos arrendados*.

1.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características en las cuales se basa la seguridad de la Información: confidencialidad, integridad y disponibilidad.

CLASIFICACIÓN Y DESCRIPCIÓN	ETIQUETADO
Restringido: Información que solo puede ser conocida y utilizada por un grupo reducido de empleados, generalmente de la Alta Dirección de Servicios Postales Nacionales S.A., y cuya divulgación o uso no autorizados podría ocasionar perdidas graves al mismo. Ej.: estrategias de negocio, estados financieros	Restringido
Confidencial: Información que solo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad. Ej.: propuestas de negocio, información de proyectos, código fuente.	Confidencial
Uso Interno: Información que puede ser conocida y utilizada por todos los empleados de la entidad y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la entidad. Ej.: Políticas, procedimientos.	Interno
Publico: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea o no sea empleado de la entidad. Ej.: Pagina Web, comunicados	Página Web

de presa.	

1.3. Rotulado de la Información

- Se definen los procedimientos para el rotulado y manejo de información, de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:
  - Copia;
  - Almacenamiento;
  - Transmisión por correo, fax, correo electrónico;
  - Transmisión oral (telefonía fija y móvil, etc.).

2. POLÍTICA DE SEGURIDAD DEL PERSONAL

2.1. Seguridad en la Definición de Roles y la Asignación de Recursos

2.1.1. Incorporación de la Seguridad en los Roles del Personal de 4-72.

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de los roles y las responsabilidades de los puestos de trabajo.

Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

2.2. Capacitación del Usuario

2.2.1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los empleados de Servicios Postales Nacionales S.A y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la entidad recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de 4-72. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

La Dirección Nacional de Gestión Humana será la encargada de coordinar las acciones de capacitación que surjan de la presente Política.

Cada año se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo con el estado del arte de ese momento.

Para estas capacitaciones se efectuarán evaluaciones de conocimiento al finalizar la capacitación sobre las políticas de seguridad de la información y se efectuará una evaluación al capacitador por medio del formato "*PR-GH-007-FR-003 Retroalimentación de la Capacitación*".

Se realizará una vez al año capacitaciones a toda la entidad sobre el presente manual.

3. POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

3.1. Seguridad para Equipos de Computo

- Todo equipo de cómputo (servidores, estaciones de trabajo, equipos portátiles, periféricos y equipo accesorio), que esté o sea conectado a la red de Servicios Postales Nacionales S.A., o aquel que en forma autónoma se tenga y que sea propiedad de los funcionarios o terceros que tengan relación con la entidad, se debe acoger a la presente política. Los ingresos de portátiles personales solo pueden ingresar a las instalaciones de SPN previa autorización de la vicepresidencia correspondiente a la cual pertenece el personal que lo va a ingresar a través de un oficio firmado por la vicepresidencia o a través de un correo electrónico enviado por el vicepresidente del área correspondiente, dirigidos al área de IT con copia al área de Seguridad.

  NOTA: *Todos los equipos personales deben ser registrados al ingresar o salir de las instalaciones de Servicios Postales Nacionales S.A.*

- Los equipos tecnológicos que se sean ingresados y no pertenezcan a SPN solo se les podrá configurar el acceso a internet, sobre la red de visitantes, de acuerdo con el tiempo estimado de uso y de acuerdo con la autorización de la vicepresidencia responsable del funcionario quien ingresa dicho elemento. Ningún equipo ajeno a SPN debe ser instalado en las instalaciones de red de la compañía, el incumplimiento de estas políticas conlleva a las sanciones disciplinarias correspondientes. En el caso de requerirse por necesidad del negocio el uso y la instalación de los equipos en la red de SPN, este deberá ser justificado y autorizado por el dueño del proceso y por la vicepresidencia responsable del proceso solicitante.

- Los Dueños de proceso/subprocesos deben informar a la Dirección Nacional de Informática y Tecnología toda instalación actualización, reubicación, reasignación y movimientos de equipos en su área, los cuales los debe efectuar únicamente el Técnico Administrativo del área de Informática y Tecnología (rol soporte).

- La Dirección Nacional de Informática y Tecnología coordina y supervisa la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y el

acondicionamiento específico a que haya lugar, siempre y cuando estos equipos sean instalados y suministrados por dicha área.

- Es responsabilidad de la Dirección Nacional de Informática y Tecnología brindar los servicios de mantenimiento básico de los equipos de cómputo, a excepción de los suministrados por terceros. Queda estrictamente prohibido dar mantenimiento a equipos de cómputo que no sean propiedad de Servicios Postales Nacionales S.A.

- Cuando se presenta un daño en el equipo asignado debe ser reportado al proceso de Informática y Tecnología, por medio del sistema de Gestion de la mesa de servicios de IT debe ingresar al link http://190.144.211.231/USDK , el usuario es el mismo del correo electrónico: Nombre.Apellido y la contraseña es la misma cuando ingresa al equipo de cómputo o comunicarse a la extensión 3030 dependiendo del inconveniente el proceso cuenta con máximo 2 días hábiles para solucionar el inconveniente o habilitar una contingencia.

- La Dirección Nacional de Informática y Tecnología es la responsable de administrar y bloquear los puertos externos para los dispositivos de almacenamiento en los equipos de cómputo.

- Toda compra de equipos de cómputo y/o periféricos a nivel de la empresa debe contar con el visto bueno del área de tecnología, esto con el fin de homologar los recursos (consumibles y partes de equipos), alineados a los elementos dispuestos por la compañía para el cumplimiento de funciones, y así puedan desempeñar y ejecutar procesos sin ningún inconveniente..

Nota: La solicitud de desbloqueo de Puertos Físicos debe realizarse a través del formato "*CP-IT-001-FR-023 Solicitud de Servicios de IT*". En caso de requerirse inmediatamente se puede generar la excepción avalada por el vicepresidente del proceso encargado.

3.2. Mantenimiento de Equipos

Se realizará el mantenimiento de los equipos para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- Someter los equipos a mantenimientos preventivos, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con

la autorización formal del Dirección Nacional de Informática y Tecnología y mantendrá un listado actualizado de los equipos con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

- Establecer que sólo los técnicos del área de IT (Rol Soporte) pueden efectuar los mantenimientos en los equipos.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- Registrar el retiro de los equipos de las instalaciones de 4-72 para su mantenimiento, para el caso de los equipos alquilados, ya que para los equipos propios los técnicos administrativos (Rol Soporte) hacen los mantenimientos respectivos.
- Eliminar la información confidencial que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo de la información.

3.2.1. Dar de Baja y/o Borrado Seguro de los Equipos.

La información puede verse comprometida por dar de baja o una reutilización descuidada del equipo. Los medios de almacenamiento conteniendo material sensible, por ejemplo, discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

3.2.1.1. Equipos Arrendados

Para los equipos arrendados la Dirección Nacional de Informática y Tecnología debe incluir cláusulas de obligatorio cumplimiento en la contratación del arrendamiento de equipos.

3.2.1.2. Equipos Propios

La Dirección Nacional de Informática y Tecnología se encargará formatear los equipos propios.

3.2.2. Políticas de Escritorios y Pantallas Limpias

Servicios Postales Nacionales S.A., adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en los equipos de cómputo, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en las cajoneras de los escritorios de trabajo cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

- Guardar bajo llave la información sensible o crítica (preferiblemente en una caja fuerte o gabinete) cuando no está en uso, especialmente cuando no hay personal en la oficina.

- Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en las áreas. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

- Proteger los puntos de recepción y envío de correspondencia y las máquinas de fax no atendidas.

- Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

- Retirar inmediatamente la información sensible o confidencial, una vez impresa.

4. POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIÓNES

4.1. Protección contra Software Malicioso

La Dirección Nacional de Informática y Tecnología definirá controles de detección y prevención para la protección contra software malicioso al igual que los implementará en la entidad.

Además, desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado en la entidad.

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinando computadoras y medios informáticos, como medida de precaución y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la entidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

	MANUAL DE INFORMÁTICA, TECNOLOGÍA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	**VERSIÓN: 4**
		CODIGO: MN-IT-019
		ACTUALIZACIÓN: Octubre/ 2018
		EMISIÓN: Enero/ 2016

4.2. Backups

Backup: “En informática, realizar una copia de seguridad o Backup (en inglés) es la operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático”

4.2.1. Residencia y Manejo de datos

1. Los sistemas de información corporativa que soportan la operación de la compañía, instalados en Data Center por el diseño y la estructura de estos aplicativos, residen en un servidor exclusivo para cada aplicación, de los cuales se efectúa un proceso de Backup del cual es responsable el proveedor del servicio, que cubre los datos, Sistema Operativo, Motor de base de datos, IIS de los diferentes ambientes de los sistemas de información. De acuerdo con el contrato que se tiene con el proveedor del servicio, este debe informar al coordinador de infraestructura y comunicaciones de Servicios Postales Nacionales S.A., por correo electrónico y también por un ticket sobre la gestión de los backups hechos en los data center.

2. La información que cuenta con respaldo es la siguiente:

a. Datos Estáticos
- Sistema operativo.
- Scripts de rutinas especiales y configuraciones.

b. Datos Dinámicos
- Bases de Datos.
- Actualización y / o modificación de las fuentes de los aplicativos.
- Datos almacenados por los usuarios (reportes, documentos, etc.)

c. Datos no almacenados
- No se realiza Backup a información con extensiones: avi, mp3, divx, mpg, wvm, o extensiones de características similares.

4.2.2. Tipos de Backups:

- **Backup Completo o full:** crea una copia de todos los archivos (Sistema Operativo, datos, bases de datos, aplicaciones, script), Ésta clase de Backup es más completa e integral, para la restauración se requiere el ultimo full Backup. La base de datos que se encuentra en el datacenter, se tiene contratado la generación de full Backup mensual. De igual manera se realiza

el full Backup mensual a las bases de datos que no se tienen contratadas en hosting.

- **Backup Incremental:** crea una copia de archivos que han cambiado (se han modificado, agregado o creado) desde el último Backup incremental, para la restauración se requiere el último Backup full y todos los incrementales que se hayan realizado. Las bases de datos que se tienen contratadas en hosting en un datacenter se tiene contratado la generación de un Backup incremental diario.

De igual manera se realizará el Backup incremental diario a las bases de datos que no se tienen contratadas en hosting.

Se definió manejar el tipo de Backup incremental diario con copia semanal y mensual Completo. Para la restauración de uno o más archivos que formen parte del Backup de Data Center, se deben tomar directamente del Backup de la fecha específica con lo cual se optimiza el tiempo de recuperación de archivos.

4.2.3. Periodicidad y Custodia del Backup de Sistemas de Información

- Para el Backup de los datos de los sistemas de información que se encuentren alojados en un centro de datos bajo contratación con un proveedor, la entidad definirá contractualmente las políticas de realización de acuerdo a los componentes de Base datos, archivos, sistema operativo y máquinas virtuales con ejecución al siguiente esquema:

  - Incremental diario
  - Full Semanal
  - Full Mensual

4.2.4. Retención

Los datos del tiempo de retención del Backup de acuerdo con el esquema son:

- Incremental diario: 1 semana
- Full Semanal: 1 mes
- Full Mensual: Duración contractual

4.2.5. Datos Críticos para Ejecución de Backups

- Datos de clientes

4.2.6. Auditoria del Proceso de Backup.

Dentro de esta política de Backup, se contempla un proceso de auditoría, en el cual se deben aplicar los siguientes parámetros:

a) Probar semestralmente la restauración de información de archivos del último Backup a full semanal y full mensual para validar la integridad del Backup.
b) Se debe efectuar una verificación de la ejecución correcta de este proceso a través de los logs de la ejecución de cada Backup.
c) Verificar que los Backups realizados se almacenen en un medio magnético y sean resguardados en un sitio diferente al datacenter principal.

4.2.7 Backups en Equipos de Computo

- La realización de las copias de seguridad de la información relevante, el usuario debe efectuarla cada mes y es responsabilidad de los funcionarios de la entidad o del personal a cargo del equipo.
- Sólo incluir en las copias archivos exclusivos de las actividades y funciones definidas según el rol desempeñado en Servicios Postales Nacionales S.A.
- Para efectuar el Backup en el equipo de cómputo, los usuarios deben ubicar los archivos en la carpeta “Disco Local C”, es importante que se cree una carpeta con el nombre del proceso involucrado más el nombre del colaborador por temas de organización y posterior ubicación de la copia de seguridad, por ejemplo: *C:\IT-Pepipo-Perez*.
- El Jefe Inmediato de proceso/subproceso debe solicitar a la Dirección Nacional de Informática y Tecnología a través de un caso en Herramienta de Gestion de la mesa de ayuda IT, la ejecución del Backup en el equipo de cómputo requerido debe ingresar la solicitud en el aplicativo de Herramienta de Gestion de la mesa de ayuda IT. El funcionario de Informática y Tecnología debe proceder con la Ejecución de Backup. Para el caso que el usuario se niegue a que efectúen el Backup en el equipo de cómputo este debe diligenciar el formato “XX-IT-001-FR-0XX Acta de Responsabilidad Ejecución de Backups en Equipos de Cómputo” asumiendo la responsabilidad de perdida de información en el equipo.
- Los Profesionales de Informática y Tecnología debe tener un inventario de los Backups ejecutados en los equipos de cómputo, deben diligenciar el formato “Inventario de Backup”.
- También se hacen Backups en los equipos cuando existen novedades de nómina con respecto a despidos o renuncias de los funcionarios de Servicios Postales Nacionales S.A.
- Como área encargada (IT) garantizamos que los medios donde se realizan los backups a solicitud de los dueños del proceso permanecerán bajo estrictas medidas de seguridad en el lugar destinado para ello.

- En caso de requerir copia del backup realizado, el dueño del proceso debe realizar la solicitud al área de IT a través de la herramienta de Gestion usada por el área de IT.

4.3. Administración de los Recursos de Red

- De acuerdo con las disposiciones de la Vicepresidencia de Soporte Corporativo, corresponde a la Dirección Nacional de Informática y Tecnología administrar, mantener, actualizar y dar soporte a la infraestructura de la red de Servicios Postales Nacionales S.A.
- A todo colaborador de 472 previa solicitud por parte del jefe de área involucrado o dueño del proceso, se le crea el usuario con las siguientes características: usuario.apellido más su contraseña, con estas credenciales el usuario podrá tener acceso a los recursos de red y a los dispositivos que se le autoricen, dependiendo de la infraestructura de los sistemas de información, en este caso directorio activo.
- Las direcciones IP internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la entidad deben ser restringidas y clasificadas como documentación confidencial.
- Todo usuario que requiera tener un acceso a los recursos de red de la entidad debe tener asociado un método de autenticación para controlar el uso de los recursos de la entidad, además deberá ser autorizado por la dirección nacional de IT previa solicitud diligenciada en la herramienta de gestión.
- Cuando sea necesaria la habilitación de puertos en el Firewall, cada Director o Jefe de Proceso por medio de la mesa de servicios de IT debe ingresar al link http://190.144.211.231/USDK, el usuario es el mismo del correo electrónico: Nombre.Apellido y la contraseña es la misma cuando ingresa al equipo de cómputo o comunicarse a las extensión 3030. La Dirección Nacional de Informática y Tecnología autoriza la activación del mismo y da el aval al Profesional de Informática y Tecnología responsable.
- Queda restringido el uso de música, películas, juegos, protectores y fondos de pantalla en los equipos de cómputo, la descarga y uso de software de libre distribución, artículos que de alguna manera vulnere lo derechos y propiedad intelectual de sus autores.

4.4. Intercambios de Información y Software

4.4.1. Políticas de Seguridad de Correo Electrónico.

- El correo electrónico institucional es una herramienta de trabajo debe ser empleado únicamente para enviar y recibir mensajes de orden institucional, no puede ser utilizado fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la entidad, además el correo no se

debe utilizar para enviar videos, música, cadenas y chistes a usuarios externos ni a colaboradores de la entidad.

- Todo mensaje sospechoso respecto de su remitente o contenido debe ser ignorado y eliminado sin abrirlo, ya que puede contener virus.
- En el buzón del correo electrónico del usuario se recomioenda que no debe superar el tamaño de 40 Gb de información, por tanto el funcionario deberá realizar depuración de información periódicamente según sea conveniente. Es responsabilidad del funcionario la información contenida del correo electrónico; el funcionario debe solicitar copia de seguridad creando la solicitud en la herramienta de Gestion de la Mesa de Ayuda de IT.
- El contenido de los mensajes debe corresponder con los “valores centrales” de la empresa, por lo tanto, no pueden ser insultantes, ofensivos, amenazantes, ni escribirse en mayúscula, subrayados o colores diferentes al azul corporativo.
- Servicios Postales Nacionales S.A. no es responsable por el contenido inapropiado de un correo entrante, pero es responsabilidad del destinatario por su reenvió a otra persona y es de su obligación remover inmediatamente de su buzón dichos correos no permitidos.
- No está permitido enviar información confidencial de la empresa a los clientes, competidores u otras entidades o personas externas sin un propósito debidamente autorizado por la alta gerencia de la entidad.
- La cuenta de correo institucional no debe ser inscrita en páginas o sitios publicitarios, de compras, deportivos, agencias matrimoniales, casinos, páginas de pornografía o a cualquier otra ajena a los fines laborales.
- No se debe enviar mensajes a todos los funcionarios, salvo que sea un asunto oficial, que involucre a toda la empresa y cuente con la autorización de Presidencia, Vicepresidentes, Secretaria General, la Dirección Gestión Humana o la Dirección Nacional de Informática y Tecnología.
- No facilitar el uso del correo electrónico a terceros para uso no autorizado por la entidad.
- No es pertinente utilizar el correo electrónico para citar a varias personas a una reunión, la forma correcta es invitar a través del calendario. La respuesta de la asistencia se debe enviar únicamente al citador y no con copia a todos los participantes.
- No se permite la utilización de fondos de ninguna clase (color, motivo o dibujo), el formato de la firma es el definido por el proceso de Marketing Estratégico.
- El tamaño de los archivos adjuntos en el correo electrónico no debe superior a 10 Megas, de ser necesario el envío de un archivo de mayor tamaño, se debe solicitar a la Dirección Nacional de Informática y Tecnología el recurso de carpetas compartidas.

4.4.2. Políticas de Adquisición de Software.

- La Dirección Nacional de Informática y Tecnología se debe acoger a la metodología de contratación establecida por la entidad para el proceso de adquisición de software esencial para el desarrollo de actividades de Servicios Postales Nacionales S.A., a través de un tercero que incluya un contrato proforma con cláusulas básicas para la protección de la información que protejan los intereses institucionales donde se fundamenten la legalidad del software incluyendo la documentación de licenciamiento.
- Todos los procesos de la entidad que requieran uso de software adicional deben contar con el visto bueno de la Dirección Nacional de Informática y Tecnología, siendo responsabilidad de cada proceso asumir el costo de dicha compra y/o arrendamiento.

4.4.3. Políticas de la Instalación de Software.

- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de información, únicamente se permite la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual y bajo aprobación de la Dirección Nacional de Informática y Tecnología.
- La Dirección Nacional de Informática y Tecnología es la responsable de brindar asesoría y supervisión para la instalación de software especializado.
- Con el propósito de proteger la integridad de los sistemas de información y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que apliquen).
- Es responsabilidad de cada funcionario la utilización de uso del software que se encuentra instalado en el equipo de cómputo asignado para el desarrollo de sus funciones
- La Dirección Nacional de Informática y Tecnología debe revisar con regularidad el software que se encuentra instalado en los equipos de cómputo de la entidad y tiene la protestad de desinstalar el software clasificado como inadecuado o que vulnere la seguridad de los recursos de red o que viole los derechos de autor.
- Los usuarios no deben introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas de información, por tanto, cada usuario es responsable de lo que pueda hacer o la información que pueda generar en los sistemas de información
- La Dirección Nacional de Informática y Tecnología es la responsable de controlar y verificar la utilización de software en los equipos de cómputo.

5. POLÍTICA DE CONTROL DE ACCESO

5.1. ADMINISTRACIÓN DE USUARIOS

5.1.1. Creación

Las autorizaciones de acceso a las aplicaciones a un usuario nuevo deben ser realizadas y firmadas dentro del formato de solicitud de IT por la vicepresidencia y/o el líder del proceso donde el funcionario desempeñará su actividad laboral según sea el caso.

Las autorizaciones deben ser remitidas a través de un caso en el Sistema de la Mesa de Servicios de IT adjuntando en el formato de solicitud de servicios de IT, diligenciado, para su configuración y aplicación en los sistemas de información de la entidad según el formato de autorización.

Los usuarios creados en los aplicativos deben ser uno por cada funcionario y se deben asignar los perfiles que a nivel de la aplicación le permitan realizar solamente las actividades asignadas.

El nombre del Usuario debe ser el mismo nombre de la cuenta de correo electrónico institucional (nombre.apellido)[1].

Todos los usuarios autorizados deben tener cuenta de correo electrónico institucional. No se permitirá la creación de usuarios genéricos, de tal forma que no sean utilizados por varias personas.

> [1]***Excepción:*** *En caso de necesitar usuarios genéricos para los procesos, estos deben tener la autorización respectiva del dueño del proceso, y de la vicepresidencia respectiva, con su debida justificación y así asegurar el buen desempeño de las funciones en las actividades que va a generar mayor valor agregado a la compañía. Además, se creará excepciones teniendo en cuenta que algunos sistemas de información tienen limitantes en la cantidad de licencias usadas por SPN. También se crearán excepciones en el caso de existir usuarios para procesos internos de la compañía como integraciones o Auditorias entre otras, estos nombres genéricos se crearán con la debida justificación, autorización del dueño del proceso solicitante, y su estructura puede ser el nombre del proceso que va usar los sistemas de información.*
>
> ***Excepción:*** *De acuerdo a la necesidad del proceso o de la compañía, y según la estructura funcional del sistema de información; un funcionario*

puede tener asociado 1 o más usuarios con diferelntes roles o perfiles, esto debidamente justificado por cada líder o dueño del proceso.

Todo usuario debe acceder siempre al sistema con el nombre de usuario que le ha sido asignado, el nombre es asignado primer nombre (.) primer apellido, de acuerdo con la estructura del Sistema de Información.

Excepción: *De acuerdo con la estructura de los sistemas de información el identificador principal para los funcionarios de SPN la estructura ideal debe ser el nombre.apellido, en el caso de clientes o aliados se podrá contemplar la estructura de nombreapellidocliente.empresacliente, si la estructura de alguno de los sistemas de información requiere que sea la identificación (Cedula o Nit) se recomienda que este sea el identificador principal para poder acceder y así hacer uso del sistema****. En caso de que la estructura de campo requiera ingresar NIT no necesariamente este debe ser de campo numérico ya que los Nit son compuestos por campos alfanuméricos ej: 12345-6.***

Nota: *Es responsabilidad de la Vicepresidencia Comercial informar a la Dirección Nacional de IT, la inactivación de Usuarios de Clientes comerciales, cuando se presente terminación del contrato comercial respectivo.*

Todo usuario de Servicios Postales Nacionales S.A., es responsable de velar por la seguridad de las contraseñas seleccionadas por él mismo para el uso de los distintos servicios y recursos ofrecidos.

La contraseña es *personal e intransferible*, por lo que *nunca debe cederse o compartirse* a terceras personas ni comunicarse por ningún medio escrito. Lo contrario supondría permitir una suplantación de personalidad.

Las contraseñas no se transmitirán de forma oral cuando exista el riesgo de que terceras personas puedan llegar a conocerlas.

Cuando un usuario olvide su contraseña se le deberá asignar otra nueva. O el software debe tener la opción para recordar la contraseña enviándola al correo electrónico registrado en el usuario de la aplicación.

La contraseña debe tener una longitud mayor o igual a siete caracteres. Se recomienda utilizar en una misma contraseña letras que alternen aleatoriamente mayúsculas y minúsculas, números y caracteres especiales.

Las contraseñas deben ser cambiadas periódicamente.

Nunca escribir la contraseña, ni almacenarla en ficheros sin encriptar, ni comunicarla en el texto de mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica.

Usuarios altos privilegios: La solicitud de usuarios de esta naturaleza por su tipo de acceso solicitado debe contener mayor control; su solicitud debe ser justificada:

- Especificar detalladamente el propósito de acceso de altos privilegios.
- Detallar el acceso solicitado a granularidad (Rol); para limitar el acceso estrictamente necesario de acuerdo con sus funciones.
- Limitar a único responsable.
- Identificación en matriz de riesgos
- Firmar carta de riesgo por la vicepresidencia y usuario responsable
- Los accesos de usuarios de altos privilegios deben ser revisados con frecuencia bimensual (cada 60 días) por el profesional de seguridad.
- El cambio, movimiento, sustitución, retiro de área (y/o de la entidad) de los usuarios con acceso de altos privilegios deben ser inmediatamente informados por Jefe inmediato, a la Dirección Nacional de IT y/o a través de la creación de un ticket en el Sistema de la Mesa de Servicios de IT.

5.1.2. Deshabilitación y/o Eliminación

Las deshabilitaciones deben ser remitidas a través de un caso en el Sistema de la Mesa de Servicios de IT por el líder de proceso. Se debe relacionar información del usuario en el formato de “CP-IT-001-FR-023 Solicitud de Servicios de IT”.

Para el caso de la cuenta de correo, informar dentro de la solicitud si la cuenta, buzón de correo requiere backup. (una vez eliminada esta información no podrá ser recuperada)

Se deben desasociar los Roles de los usuarios y bloquear la cuenta a nivel de las Bases de Datos, cambiar contraseña y/o eliminar perfiles en la aplicación.

Eliminar cuentas no utilizadas en los sistemas de información y red por más de 90 días.

Se bloquearán las cuentas en los sistemas de información y red no utilizadas por más de 30 días.

5.1.3. Modificación

Bloqueo Intencional: Este bloqueo es solicitado por el Dueño del Proceso/Subproceso para suspender temporalmente los accesos a un sistema de

información bien sea por novedades como: Vacaciones, licencias, incapacidades u otro tramite de suspensión a un usuario.

Desbloqueo de Cuentas: Este desbloqueo de claves de acceso a los sistemas de información se da cuando el usuario ha olvidado la clave o por intentos fallidos o por expiración de la clave. Para Solicitar el desbloqueo de la cuenta el dueño del de las credenciales de usuario se debe realizar la solicitud a través de la herramienta de Gestion de la mesa de Servicios, la mesa de servicios procederá a atender dicho requerimiento y una vez gestionado procederá a informar al usuario quien realiza la solicitud, a su cuenta de correo institucional.

Nota: En caso de tener bloqueado el acceso a la herramienta de Gestion de Servicios de la mesa de servicios, se debe proceder con solicitud en Herramienta de Gestion de la mesa de ayuda IT por parte del jefe Inmediato del funcionario.

5.1.4. Pasos para la Administración de Cuentas de Usuario

Responsable: Dueño de Proceso/Subproceso

- Cada Jefe Inmediato o Dueño del proceso deberá realizar y autorizar las diferentes solicitudes de los sistemas de Información de SPN.
- Realizar la solicitud de creación, activación o modificación en el sistema de información por medio del Formato de “CP-IT-001-FR-023 Solicitud de Servicios de IT”, esta solicitud debe ser por parte de Vicepresidentes, Jefes de Oficinas Asesoras, Directores, Gerentes o Jefes Nacionales, o personal delegado por el dueño del proceso.
- El dueño del proceso o su delegado debe Gestionar las firmas de autorización en dicho formato, definido por ese dueño de proceso/subproceso.

Responsable: Asistente de la Dirección Nacional de Informática y Tecnología

- Verificar e informar a la Dirección Nacional de IT que el trámite solicitado por el personal respectivo se encuentra autorizado para realizar estas solicitudes.

Responsable: Técnico de la Mesa de Servicios y Profesional IT

- Verificar que exista un caso en el aplicativo de la Mesa de Servicios de IT adjuntando el formato con las respectivas firmas de autorización.
- Recibir el caso con el requerimiento y verificar que el formato este con las firmas de autorización completas.
- Verificar el tipo de solicitud.

- Escalar el caso al grupo de IT correspondiente según el tipo de solicitud.
- Realizar la gestión según la solicitud:

Creación: Realiza la creación del nuevo usuario en el sistema de información.

Activación: Realiza la activación de usuario en el caso de reingresar a la compañía, esto en el sistema de información.

Modificación: Realiza la modificación de perfiles o de accesos, de acuerdo con la justificación de la solicitud. La revisión de los privilegios asociados al perfil del usuario para la modificación debe ser responsabilidad de los dueños de procesos, esta revisión debe realizarse mínimo anual.

- Cerrar el caso en el aplicativo de la Mesa de Servicios de IT.
- Informar al usuario la solución a la solicitud mediante la respuesta en el sistema de gestion de casos.

5.1.5. Pasos para la Inactivacion de Cuentas de Usuario

a) El dueño de proceso a solicitud mediante un caso en la herramienta de Servicios de Mesa de Ayuda informe de la Inactivacion de una o mas cuentas.
b) Mediante tramite del paz y salvo en el caso de terminación de vinculo laboral con la empresa.
c) Mediante solicitud del área de Gestion Humana según listado reportado periódicamente (cada vez que exista terminación del vinculo laboral) cuando se presenten terminación contractual del personal o funcionarios de la empresa.

Para los casos mencionados anteriormente, se debe proceder de la siguiente forma.

Para el Numeral a)

Responsable: Dueño de Proceso/Subproceso

- Cada Jefe Inmediato o Dueño del proceso deberá realizar y autorizar las diferentes solicitudes de los sistemas de Información de SPN.

- Realizar la solicitud de Inactivacion en el sistema de información por medio de la herramienta de Gestion de la mesa de Ayuda.

Responsable: Técnico de la Mesa de Servicios y Profesional IT

- Verificar que exista un caso en el aplicativo de la Mesa de Servicios de IT.
- Recibir el caso con el requerimiento
- Escalar el caso al grupo de IT correspondiente según el tipo de solicitud.

- Realizar la gestión según la solicitud:

  Inactivación: Realiza la inactivación del usuario y desasociar los roles y programas en el sistema de información.

- Cerrar el caso en el aplicativo de la Mesa de Servicios de IT.
- Informar al usuario la solución a la solicitud mediante la respuesta en el sistema de gestión de casos.

Para el Numeral b)

Responsable: Funcionario a cargo de la Cuentas de Usuario

- Realizar la gestión de Firmas del paz y salvo respectivo.
- Informar a la mesa y presentar el paz y salvo para realizar la respectiva inactivación.

Responsable: Técnico de la Mesa de Servicios y Profesional IT

- Revisar el paz y salvo e inactivar todos los accesos y cuentas de usuarios a los diferentes sistemas de información asignados.
- Realizar la gestión según la solicitud:

  Inactivación: Realiza la inactivación del usuario y desasociar los roles y programas en el sistema de información.

- Se da Visto buenos sobre el Paz y Salvo del funcionario que reporta..
- Informar al usuario la solución a la solicitud.

Responsable: Dirección Nacional de IT

- Revisar que el paz y salvo contenga los Visto Buenos del profesional de It y de la mesa de servicios para proceder a dar el VB correspondiente.

Para el Numeral c)

Responsable: Área de Gestion Humana

- Informar mediante correo electrónico o en físico a la Dirección Nacional de IT, el listado del personal que presenta terminación de Vínculo Laboral con la Compañía, este reporte debe ser enviado cada vez que se presenten terminaciones laborales.

Responsable: Técnico de la Mesa de Servicios y Profesional IT

- Revisar el reporte enviado por el área de Gestion Humana o por la Dirección Nacional de IT e inactivar todos los accesos y cuentas de usuarios a los diferentes sistemas de información asignados.

- Realizar la gestión según la solicitud:

  Inactivación: Realiza la inactivación del usuario y desasociar los roles y programas en el sistema de información.

Excepción: De acuerdo a la estructura de seguridad de los sistemas de información, la cuenta de usuario se inactivará automáticamente de acuerdo al tiempo parametrizado en dicho sistema de información.

5.1.6. Depuración de Usuarios

Cada dueño de proceso en los módulos usados en los sistemas de información es responsable de realizar la revisión periódica, recomendada 2 veces al año, y realizar la solicitud de esta depuración mediante oficio por escrito, anexando el listado de los usuarios a depurar, al área de Informática y Tecnología, para así poder realizar y atender la Gestión respectiva.

5.1.7. Definición de Roles

- Las autorizaciones para la creación de un nuevo rol en las aplicaciones implementadas dentro de la entidad deben ser realizadas y firmadas dentro del formato de solicitud de IT por la vicepresidencia y/o gerente de regional y/o director de proceso donde el funcionario desempeñará su actividad laboral según sea el caso.
- La autorización para modificación de un rol existente de una regional debe ir con la aprobación de los gerentes de regionales. De igual manera las autorizaciones para la modificación de un rol de la regional Centro A debe ser aprobada por el Jefe de Proceso al cual está asignado el rol.
- Las inactivaciones de roles deben ser remitidas a través de un caso en el Sistema de la Mesa de Servicios de IT por el vicepresidente y/o el gerente de regional, se debe diligenciar el formato de “CP-IT-001-FR-023 Solicitud de Servicios de IT”, y diligenciar un caso en el sistema de la mesa de servicios de TI.
- Las autorizaciones deben ser remitidas a través de un caso en el Sistema de la Mesa de Servicios de IT adjuntando en el formato de solicitud de servicios de IT, diligenciado, para su configuración y aplicación en los sistemas de información de la entidad según el formato de autorización.
- No se permitirá la modificación de roles que pertenezcan a otros procesos.

Excepción: *En caso de necesitar roles diferentes en las regionales, estos deben tener la autorización únicamente del gerente de regional, con su debida justificación y quien*

será el responsable por velar por el buen desempeño de las funciones en las actividades que va a generar mayor valor agregado a la compañía.

5.2. ADMINISTRACIÓN SISTEMAS DE INFORMACIÓN Y BASE DE DATOS

La administración de los sistemas de información principales se encuentra tercerizado a través de la contratación de alojamiento en modalidad de nube privada, hosting físico y/o hosting virtual, centralizado en un centro de datos que permita la operación a nivel nacional de los sistemas de información críticos del negocio incluyendo los servicios de gestión, administración, monitoreo, disponibilidad de las aplicaciones, almacenamiento, licenciamiento, administración de los sistemas operativos y motores de bases de datos, copias de respaldo (Backups) de la plataforma tecnológica y de la información de Servicios Postales Nacionales S.A.

5.2.1. Alcance de la Administración

El alcance de la tercerización está enmarcado a las siguientes actividades: administración y monitoreo de dispositivos físicos de los servidores, instalación, administración y monitoreo del comportamiento de los sistemas operativos, instalación, administración y monitoreo de comportamiento y verificación de la base de datos, administración y monitoreo de las máquinas virtuales, identificación de problemas potenciales que afecten la disponibilidad o el desempeño del sistema operativo y base de datos. Atención de fallas y ejecución de planes preventivos de acuerdo procedimientos definidos para ello. Análisis de datos históricos para realizar proyecciones de capacidad requerida en la Infraestructura de la solución.

5.2.2. Servicios Cubiertos en la Administración

Los niveles de administración y verificación de los sistemas de información están establecidos de acuerdo con lo siguiente:

1. Espacio de filesystems
2. Recursos de memoria y I/O Finalización de los Backups
3. Objetos Inválidos
4. Índices
5. Archivos de logs
6. Conteo de sesiones
7. Tablespace o filegroups no disponibles.
8. Disponibilidad del Listener, de la base de datos.

9. Balanceo de conexiones y failover para cluster.
10. Procesos background de bases de datos.
11. Top five de Consultas pesadas.
12. Bloqueos de base de datos
13. Objetos fragmentados
14. Ejecución de tareas programadas y scripts definidos en la línea base o inventario inicial.
15. Instalación de nuevos componentes de software (actualizaciones periódicas)
16. Monitoreo y administración de la seguridad de las bases de datos (incorporación y eliminación de usuarios, administración de espacios de disco o cuotas, auditorias y revisiones periódicas)
17. Control y reasignación de claves a usuarios del sistema.
18. Monitoreo del rendimiento de la base de datos y efectuar ajustes de sintonización (tunning) cuando se requiera.
19. Ejecutar una estrategia efectiva de respaldos y recuperación de los mismos para garantizar una estabilidad de la información guardada. Los respaldos y la recuperación están asociados a la base de datos, objetos y usuarios.
20. Instalar, actualizar, configurar, indexar las bases de datos en los servidores, bajo las políticas y procedimientos para manejo de cambios y problemas que se generen.
21. Monitorear, Analizar y solucionar fallas, caídas y bloqueos de las bases de datos.
22. Mantener las estructuras de las bases de datos en los estados óptimos de espacio disponible y balance de los índices.
23. Verificación diaria de disponibilidad y control de bloqueos del sistema.
24. Administración de restauración de backups de Base de Datos de las plataformas administradas.
25. Registro de Eventos de cambio en la Base de Datos e Instancias.
26. Revisión y diagnóstico de los Archivos de LOG.
27. Control de rendimiento de las Instancias de Base de Datos.
28. Control de Seguimiento de Errores a nivel de bases de datos.
29. Verificación de correcta ejecución de la de Información de Respaldo.
30. Reorganización de los objetos de Bases de Datos (tablespaces, tablas, índices, usuarios y otros).
31. Realizar el cálculo de las estadísticas para las tablas e índices.
32. Mantener las actualizaciones de las versiones de las Bases de Datos.
33. Realizar el control de Ejecución de scripts propias de la Administración.
34. Realizar el control de Creación y modificación de objetos.
35. Mantenimiento de objetos de programación en las bases de datos productivas, triggers, store procederes, vistas, funciones, paquetes.
36. Administración de los ambientes de bases de datos de desarrollo, producción y pruebas y otros que se generen en la compañía.

37. Mantener el sistema operativo en cada máquina que haga parte de la arquitectura.
38. Mantener la protección del sistema operativo de cada máquina que haga parte de la arquitectura.
39. Realizar monitoreo de la detención y reinicio de servicios críticos y de los sistemas operativos.
40. Realizar escaneo de vulnerabilidades de seguridad sobre el sistema operativo.
41. Reportar los eventos y alarmas presentados en el sistema operativo, y mantener un histórico de su disponibilidad y desempeño. Las variables mínimas por monitorear con umbrales son:

    - Disco.
    - Memoria.
    - Procesamiento. Uso de red.

42. Realizar el Monitoreo de los logs.
43. Realizar el monitoreo servicios críticos.
44. Realizar el monitoreo de disponibilidad de las aplicaciones
45. Administración de usuarios:
    - Creación de usuarios
    - Desbloqueo de usuarios
    - Cambio de contraseñas de usuario
46. Ejecución de actividades periódicas:
    - Ejecución y reporte de resultados de tareas periódicas de mantenimiento de infraestructura o de procesos de negocio de los clientes (tareas programadas)
47. Ejecución de mantenimientos programados:
    - Ejecución de ventanas de mantenimiento de actualizaciones (los administradores definen previamente que actualizaciones se deben aplicar)
48. Análisis de consumo de recursos (mantenimientos)
49. Los administradores deben presentar un análisis sobre los reportes mensuales, con las recomendaciones que apliquen para optimizar el uso de los recursos de la infraestructura existente.

5.2.3. Controles

- Revisión de informes de gestión entregados por el tercero. Reuniones técnicas periódicas con el proveedor.
- Reuniones administrativas periódicas con el proveedor (revisión de ANS y cumplimiento).
- Ejecución de auditorías semestrales de cumplimiento en lo servicios contratos

5.3. Administración de Usuarios y Contraseñas

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.

- Los usuarios no deben intentar sobrepasar los controles de los sistemas, con software que intente examinar los computadores y redes de la entidad en busca de vulnerar la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica. Estas actividades deben ser expresamente controladas, monitoreadas por la Dirección Nacional de Informática y Tecnología
- Los colaboradores no deben suministrar las credenciales de autenticación de red de la entidad a ningún ente externo, sin las autorizaciones respectivas.
- Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos. La información contenida en los equipos portátiles es de absoluta reserva y confidencialidad. El portador del equipo portátil es responsable del uso inapropiado que se le pueda dar.
- Los equipos de cómputo de la entidad no pueden ser accedidos, modificados y manipulados por terceros sin previa autorización de la Dirección Nacional de Informática y Tecnología.
- La Dirección Nacional de Informática y Tecnología es responsable de proporcionar a los usuarios el acceso a los recursos informáticos de acuerdo con las responsabilidades de los mismos.
- Cada usuario es responsable por el uso que se les otorgue a los sistemas de información y plataforma tecnológica que le sea proporcionado por la Dirección Nacional de Informática y Tecnología.
- Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario.
- El usuario con servicio a los accesos remotos de los recursos informáticos disponibles debe sujetarse a las políticas de seguridad informática de la entidad.

  Nota: La solicitud de accesos remotos debe realizarse a través del formato "*CP-IT-001-FR-023 Solicitud de Servicios de IT*"

- La Dirección Nacional de Informática y Tecnología es responsable de administrar el control y la restricción de acceso a internet por ejemplo páginas de redes sociales, páginas de videos, pornografía, páginas de entretenimiento o a cualquier otra página web ajena a los fines laborales.

  Nota: La solicitud para el ingreso a las páginas de internet restringidas debe realizarse a través del formato "*CP-IT-001-FR-023 Solicitud de Servicios de IT*" y debe ser aprobada por la Presidencia o por quien ésta delegue.

- El material que aparezca en el portal corporativo de Servicios Postales Nacionales S.A. debe ser aprobado por la Presidencia, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material de publicación o impreso).
- La Dirección Nacional de Informática y Tecnología tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información.

5.4. Control de Acceso a los Sistemas de Información

5.4.1. Acciones para Construir Contraseñas Seguras:

- Todo usuario debe acceder siempre al sistema con el *usuario (User-ID) que le ha sido asignado, el nombre ideal asignado es primer nombre el punto (.) y primer apellido, teniendo en cuenta la estructura del Sistema de Información, en algunos sistemas de información el usuario asignado está definido por el número de cedula en el caso de funcionarios de SPN o el número de Nit en caso de Clientes*
- Todo usuario de Servicios Postales Nacionales S.A., es responsable de velar por la seguridad de las contraseñas seleccionadas por él mismo, para el uso de los distintos servicios y recursos ofrecidos.
- Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el User-ID de otros usuarios. Las contraseñas son personales e intransferibles. Lo contrario supondría permitir una suplantación de personalidad.
- Las contraseñas no se transmitirán de forma oral cuando exista el riesgo de que terceras personas puedan llegar a conocerlas.
- Cuando un usuario olvide su contraseña se le deberá asignar otra nueva a través de una solicitud por parte del funcionario que la olvidó, esto a través de un caso en el sistema de Gestión. O el software debe tener la opción para recordar la contraseña, enviándola por correo electrónico al usuario registrado en la aplicación.
- La contraseña debe tener una longitud mayor o igual a siete caracteres. Se recomienda utilizar en una misma contraseña letras que alternen aleatoriamente mayúsculas y minúsculas, números y caracteres especiales.
- Las contraseñas deben ser cambiadas periódicamente, como buena práctica de seguridad, para evitar que el usuario sea vulnerado.
- La Dirección Nacional de Informática y Tecnología informará a sus usuarios de todas estas políticas y velará por su cumplimiento.
- Cuando un usuario se traslade de proceso, conserva su nombre y contraseña, aunque trabaje en otro lugar.
- Las contraseñas no se comunicarán en conversaciones telefónicas.

- El funcionario a cargo de sus credenciales nunca escribirá la contraseña, ni almacenarla en ficheros sin cifrar, ni comunicarla en el texto de mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica.

5.4.2. Usuarios sistemas de información

- El usuario dispone de un **identificador de usuario** y de una **contraseña** (o clave) que son personales e intransferibles. Estos son almacenados cifrados en la base de datos de los sistemas de información para su uso como método de autentificación, identificación del usuario que le permite el acceso.
- La Dirección Nacional de Informática y Tecnología velará por la distribución segura de las contraseñas.
- El uso de los servicios, así como la utilización, conservación y comunicación de la información que se obtiene utilizando el identificador de usuario debe limitarse a las actividades misionales que el usuario tenga encomendadas y ser protegida contra el acceso de personas no autorizadas.
- Contraseñas de acceso:

    - Está **prohibida** la divulgación de la clave a otras personas, tengan o no relación con Servicios Postales Nacionales S.A. El usuario será el responsable de todas las actividades realizadas sobre el sistema con su usuario identificador, de ahí la importancia de mantener el carácter privado de la clave como forma de garantizar el carácter personal e intransferible de ésta.
    - La contraseña debe tener una longitud mayor o igual a siete caracteres.
    - El propietario **deberá** proceder al cambio de contraseña de forma periódica y de forma inmediata si tuviere indicios de que la misma puede ser conocida por terceras personas.
    - En el momento del cambio, no estará permitida la reutilización del valor empleado para las últimas claves, según la antigüedad que se especifique.
    - Tras utilizar la aplicación con el usuario y contraseña, éste ha de cerrar la sesión mediante las opciones disponibles para evitar que otro usuario pueda acceder posteriormente a los servicios desde su puesto de trabajo.

- La violación o intento de violación de la seguridad de los sistemas de información o red pueden incurrir en responsabilidades civiles y criminales. Servicios Postales Nacionales S.A., colaborará al máximo de sus posibilidades para investigar este tipo de actos, incluyendo la cooperación con la Justicia.

- El incumplimiento de la presente normativa supondrá la cancelación inmediata del acceso del usuario sin perjuicio de otras medidas que se puedan emprender en el ámbito funcional.
- Según configuración dentro de los sistemas de información, esta obliga cambio de contraseña periódicamente entre 1 y 3 meses.

5.4.3. Acciones que deben evitarse en la gestión de contraseñas seguras:

- Se debe evitar utilizar la misma contraseña siempre en todas las aplicaciones.
- Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf”, las típicas en numeración: “1234” ó “98765”)
- No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
- No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio equipo de cómputo o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del equipo de cómputo).
- No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- Las aplicaciones deben bloquear con tres intentos de acceso.
- Las aplicaciones deben tener opción para recordación de contraseña, a un correo definido al usuario.
- Evite la utilización de sus credenciales de usuario de la entidad en equipos de carácter público, sitios de internet, cafés de internet, etc. donde desconozca su nivel de seguridad y control.
- Cambiar las contraseñas por defecto proporcionadas por desarrolladores o fabricantes.
- Con el objetivo de controlar los accesos no autorizados La Dirección Nacional de Informática y Tecnología efectúa revisiones periódicas a los Sistemas de Información con el objetivo de:
  - Inhabilitar cuentas inactivas por más de un período no mayor a 60 días.
  - Eliminar cuentas inactivas por más de un período no mayor a 90 días. En el caso de existir excepciones, deben ser justificadas y aprobadas.

- La Dirección de Gestión Humana debe informar a la Dirección Nacional de Informática y Tecnología periódicamente las novedades (Despidos o Renuncias) que se presenten con respecto al personal de Servicios Postales Nacionales S.A para inactivar las cuentas de correo o inactivar al usuario de algún sistema de información en el cual este creado.

- No debe concederse cuentas de usuario a personas que no tengan vínculos laborales con la entidad a menos, de que estén debidamente autorizados por la Dirección Nacional de Informática y Tecnología, en cuyo caso la cuenta no debe estar activa tiempo finito.
- La solicitud de una cuenta de usuario ya sea para tener acceso al correo electrónico o aun sistema de información, el cambio de privilegios o el bloqueo de la misma, debe tener el aval de La Dirección Nacional de Gestión Humana por medio de la mesa de servicios de IT debe ingresar al link http://190.144.211.231/USDK adjuntando el formato de solicitud de servicios de IT con sus VB respectivos, el usuario para ingresar a la herramienta de Gestion es el mismo del correo electrónico: Nombre.Apellido y la contraseña es la misma cuando ingresa al equipo de cómputo o comunicarse a las extensión 3030.

5.5. Custodia de Contraseñas de Perfil de Alto Privilegio

La contraseña de perfil de Alto Privilegio debe cumplir con el numeral 5.3 y 5.4 del presente manual.

La custodia de dicha contraseña debe ser almacenada físicamente en un sobre sellado, guardada y custodiada en la caja fuerte de la dirección Nacional de IT. En el caso de ser requerida se debe dejar constancia por escrito de su uso entrega y responsable del uso.

5.6. Horario de Uso de las Credenciales

El horario de uso de las credenciales en los diferentes sistemas de información deberá ser recomendado en horario laboral, sin embargo, dependiendo de la necesidad de dicho uso, se ajustaran a su respectivo horario, en el caso de los sistemas de información de la operación, este debe ser en un horario 7 x 24 (7 días a la semana, 24 horas al día).

Excepción: De acuerdo a la necesidad de la compañía, se podrá ampliar el horario del uso de cualquier sistema de información, debidamente justificado y aprobado por el dueño del proceso y la vicepresidencia del proceso solicitante o quien Presidencia delegue; esta solicitud deberá ser enviada por escrito y firmada o mediante un correo electrónico y un caso en la herramienta de Gestion de mesa de servicio, por parte de la vicepresidencia del proceso solicitante o el delegado de Presidencia, a la dirección nacional de IT.

5.7. Logs de Auditorias

Una vez definida la estructura de auditoria de los sistemas de información, existirá por lo menos en los sistemas CORE de la compañía, un modulo que permita realizar seguimiento y auditorias a los procesamientos internos de la información dentro de cada aplicativo.

5.7.1. Administración de los Logs de Auditorias y sus responsables.

Teniendo en cuenta que la compañía no cuenta con certificación de la norma ISO 27001, esta administración de logs no tendrá una metodología definida como lo exige la norma.

El área de IT es el área responsable de administrar los logs respectivos frente a la necesidad de cualquier auditoria llevada a cabo por las áreas de control interno de la compañía y de los diferentes entes de control externo.

Además, se expondrá o se dará acceso a quien se vea conveniente y a solicitud para que se revisen dichos logs, el módulo estará disponible para que cada líder del proceso quien considere necesario realizarlo y mediante solicitud según la estructura necesaria definida solicitada al área de IT pueda hacer seguimiento y control según sus actividades, funciones y responsabilidades que sean acordes a su cargo.

Es necesario e importante que el área de Control Interno Audite y Evalúe constantemente dichos logs, esto con el fin de prevenir cualquier circunstancia que pueda afectar la operación de la compañía.

Es necesario e importante también que el área de Operaciones y Gerencias Regionales monitoreen constantemente dichos logs, esto con el fin de prevenir cualquier circunstancia que pueda afectar la operación de la compañía.

Los archivos de logs generados serán entregados por parte del área de IT a quien haga la solicitud debidamente justificada y mediante los procedimientos establecidos por IT (Caso en Herramienta de Gestión de la mesa de ayuda IT justificando la necesidad de los reportes de logs) a través de archivos planos para su respectiva interpretación y revisión.

El backup o copia de seguridad de los logs de auditoria, están cubiertos contractualmente por el proveedor de infraestructura, y se hacen backups a diario.

6. POLÍTICAS DE UTILIZACIÓN DE CONTROLES CRIPTOGRÁFICOS

Se deben usar sistemas y técnicas criptográficas para proteger la contraseña de usuarios, cuando otras medidas y controles no proporcionen la protección adecuada.

Objetivo: Proteger la confidencialidad, autenticidad e integridad de las contraseñas de los usuarios de las aplicaciones.

Alcance: Esta política se aplica a todos los empleados, contratistas y clientes para las aplicaciones de Sipost y Seven.

6.1. Uso de los controles criptográficos

Servicios Postales Nacionales S.A., existe una política de uso de las medidas Criptográficas para proteger la información.

La política debe considerar lo siguiente:

- Para Sipost utilizar funciones de cifrado provistas por .NET (MD5), más las implementadas por el SSL.

6.2. Cifrado Unidireccional

Las funciones HASH o resumen se basan en realizar un cálculo que devuelve un valor de longitud fija sobre el texto que deseamos cifrar.

Este cifrado no es reversible, y normalmente se utiliza para almacenar claves de usuario (al realizar la verificación de identidad, se calcula el valor HASH de la contraseña introducida, y si coincide con el HASH de la almacenada, se considera correcta). La gran ventaja de un cifrado HASH es que, accediendo, por ejemplo, a la tabla de usuario/contraseña almacenada en un directorio la información no es comprometedora.

También podemos agregar un nivel de seguridad a nuestras bases de datos con este cifrado unidireccional. Incluyendo una tabla maestra de nombre-HASH también protegeremos la información, aunque no es nada que no nos resuelvan los identificadores largos de SQL Server (y resulta más eficiente).

a) Un enfoque de gestión del uso de las medidas criptográficas a través de la entidad, incluyendo los principios generales en base a los cuales se debería proteger la información del negocio.

b) Basados en la evaluación del proceso de riesgos y cumplimiento, el nivel requerido de protección debe ser identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido.

c) El uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación.

d) Un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves;

e) Las aplicaciones implementadas en Servicios Postales Nacionales S.A., deben definir los roles y responsabilidades de cada aplicación, las cuales deben requerir:

1) La implementación de la política.
2) La gestión de claves, incluyendo la generación de claves

f) Las normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus).

Los controles criptográficos deben ser utilizados para alcanzar diferentes objetivos de seguridad como por ejemplo:

a) Confidencialidad: utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.

b) Integridad/autenticidad: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.

c) No repudio: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

6.3. Gestión de claves

La gestión de claves debe apoyar el uso de las técnicas criptográficas en la organización.

Se debe proteger todos los tipos de claves de su modificación o destrucción. Con este fin también deben usarse técnicas criptográficas.

El sistema de gestión de claves se debe basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) Generar claves para distintos sistemas criptográficos y distintas aplicaciones.
b) Generar y obtener certificados de clave pública.

c) Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.

d) Cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse.
e) Revocar claves, incluyendo la forma de desactivarlas o retirarlas, por ejemplo, cuando tienen problemas o el usuario deja la organización (en cuyo caso las claves también se desactivan);

f) Recuperar claves que se han perdido o corrompido como parte de la gestión.
g) Continuidad del negocio, por ejemplo, para recuperar la información cifrada.
h) Inactivar claves.

i) Hacer seguimiento y auditorias de las actividades relacionadas con la gestión de las claves.

Para reducir la probabilidad de comprometer las claves, se debe definir fechas de activación y desactivación para que sólo puedan utilizarse durante un periodo limitado. Este debería depender de las circunstancias del uso de las medidas de control criptográficas y del riesgo percibido.

Servicios Postales Nacionales S.A., debe contratar un proveedor de servicios criptográficos (por ejemplo, una autoridad certificadora) para cifrar los datos sensibles del negocio.

7. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Un incidente, es todo aquello que impacta o afecta negativamente la confidencialidad, integridad, y disponibilidad, de la información.

La información y los sistemas de información de la entidad son considerados activos de la entidad y deben disponerse los recursos necesarios para brindar una apropiada gestión de incidentes de seguridad.

La Dirección de la entidad reconoce la importancia de gestionar los incidentes de seguridad de la información, y la adopción de medidas de seguridad eficientes para proteger sus activos de información críticos.

La Dirección de la entidad declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de gestión de incidentes de seguridad, y protección de datos personales.

Difundir la presente política a todo el personal de la entidad, independiente del cargo que desempeñe y de su situación contractual.

Todo el personal de la entidad es responsable por:

- Dar cumplimiento a la presente política, independiente del cargo que desempeñe y de su situación contractual.
- Reportar oportunamente los eventos de seguridad que detecte a la mesa de servicios de la entidad.
- Garantizar la confidencialidad, integridad, disponibilidad de la información de cualquier tipo en el ejercicio de sus funciones.
- Documentar y clasificar los incidentes de acuerdo con las indicaciones del proceso de gestión de incidentes.

7.1. Notificación de incidentes de seguridad de la información

Para la administración de las brechas de seguridad o indicio de uso inadecuado de los servicios de la red (internet, correo, etc.), sistemas de información, datos e información de la entidad, infraestructura tecnológica en cualquier nivel jerárquico deberá ser comunicado por el colaborador que la detecta, en forma inmediata y confidencial, como una afectación o incidente de seguridad.

Para la notificación de incidentes relacionados con seguridad de la información el usuario afectado y/o espectador, debe remitir el formato en documento adjunto "*XX-IT-0XX-FR-XXX Notificación de Incidentes de Seguridad de la Información*" en

herramienta de la Mesa de Servicios de IT y comunicarse vía telefónica a la mesa de servicio de Servicios Postales Nacionales S.A., para comunicar lo sucedido.

La información suministrada será manipulada estrictamente de carácter confidencial y posteriormente validada por el grupo de especialistas de la Dirección Nacional de Informática y Tecnología, para evaluar la existencia de una violación de algunos de los controles expresados en la política o clasificado como violación la integridad, confidencialidad, disponibilidad de uno o algunos compontes tecnológicos de la entidad.

7.2. CONTROL DE CAMBIOS DE LOS SISTEMAS DE INFORMACIÓN

Contemplar un cronograma con las publicaciones de control de cambios en los sistemas de información, diligenciar completamente el formato ”MN-IT-019-FR-002 Cronograma Publicaciones de Control de Cambios en Sistemas de Información”

Para realizar publicación en producción según fechas predefinidas; deben asistir todos los interesados y/o afectados a la reunión

Los proponentes del cambio deben coordinar los recursos de IT y del negocio para la realización de las pruebas.

Para el Comité se debe llevar diligenciado completamente el formato MN-IT-019-FR-001 Solicitud de Control de Cambios y Publicaciones y creado el cambio en la herramienta de gestión, para su aprobación.

El proceso de Operaciones debe apoyar la ejecución de pruebas de atención incidentes y nuevos requerimientos.

7.2.1. Tipos de Cambios

Los tipos de cambio a los sistemas de información se detallan a continuación:

Tipo de Cambio	Descripción
Requerimiento de negocio	Se requiere una nueva funcionalidad para un servicio existente o un nuevo servicio, con la justificación de negocio correspondiente, generalmente corresponde a solicitudes de nuevas funcionalidades.
Incidente/problema	El cambio tiene como objetivo implantar una solución temporal o eliminar la causa raíz de algún problema detectado o incidente reportado.
Legislación	Cambios en la legislación y normativas obligan a efectuar cambios en los sistemas de información.

7.2.2. Roles y Responsabilidades

Los roles de los encargados de realizar las actividades relacionadas con administración de cambios y configuraciones y sus responsabilidades se describen a continuación:

Roles	Responsabilidades
Gerente de Proyectos IT/Gerente de Operaciones IT	Solicitante del cambio Preparación y presentación de entregables Proveer una retroalimentación una vez implantado el cambio

Administrador de Aplicaciones y BD	Informa el estado o evolución de los cambios Participa del comité de cambios aportando su conocimiento del negocio para establecer el impacto de los cambios Identifica problemas presentados e informa al comité Notifica a las áreas involucradas todas las publicaciones que se hagan en los sistemas de información. Solicita el paso a producción de los incidentes
Líder Funcional	Solicita el paso a producción Efectúa la entrega de los requisitos para el paso a producción Prueba que el cambio funcione correctamente Certifica con pruebas transversales el funcionamiento de los cambios en el ambiente de pruebas. Planea los cambios aprobados Capacita a los usuarios finales y a los funcionarios de IT.

7.2.3. Integrantes sobre la Gestión del Control de Cambios y Publicaciones

- Director Nacional de IT
- Gerente de Operaciones IT Líder de Proyectos SPN
- Líder de Aplicaciones Gerente de Proyectos Líder de Servicios de IT
- Líder de Administración de Plataformas Líder Mesa de Servicio
- Gerente de Proyecto del Proveedor Arquitecto de Soluciones SPN
- Técnico Funcional SPN

7.2.4. Pasos para el Control de Cambios en los Sistemas de Información

Responsable: Gerente de Proyectos de IT y/o Gerente de Operaciones IT

a. Solicitar el paso a producción del requerimiento, incidente o nueva aplicación.

Responsable: Administrador de Aplicaciones y BD

b. Verificar las solicitudes de acuerdo con los tipos de necesidades, nuevos requerimientos y/o atención de incidentes. (Mínimo 2 veces al mes).
c. Autorizar el paso a producción y determinar la fecha en que se efectuará la publicación.

Responsable: Líder de proyectos y/o Administrador de Aplicaciones y BD

d. Informar a las áreas involucradas sobre la publicación (fecha, hora y los cambios) que se harán en el sistema. (debe informar 48 horas antes de publicar los cambios en el ambiente de producción)
e. Coordinar con el proveedor y datacenter la correcta publicación de los cambios en el ambiente de producción.
f. Hacer seguimiento y control de los cambios hechos en el sistema para que no existan inconvenientes.

Responsable: Coordinador(a) de la Mesa de Servicio de IT

g. Enviar notificación a los procesos de negocio, informando los tiempos de indisponibilidad del servicio.

7.3. GESTIÓN DE PROYECTOS

a. La Dirección Nacional de Informática y Tecnología cataloga sus proyectos de solución de información en tres tipos, los cuales pueden ser entregados para su operación en producción:
b. Proyecto A: Son los nuevos sistemas de información o modificaciones sobre sistemas existentes de alto impacto en el negocio, cuyo alcance se desarrolla en una duración superior a 6 meses; requiriendo tiempo completo (más del 75%) del líder del proyecto asignado.
c. Proyecto B: Son los nuevos sistemas de información o modificaciones sobre sistemas existentes, cuyo alcance se desarrolla

en una duración entre 3 y 6 meses, interactuando con dos o más sistema de información; requiriendo medio tiempo (50%) del líder del proyecto asignado.

d. Proyecto C: Son las modificaciones y soluciones de incidentes a los sistemas de información existentes, cuyo alcance se desarrolla en una duración entre 1 y 3 meses; requiriendo un cuarto del tiempo (entre 10% y 25%) del líder del proyecto asignado.
e. Estas definiciones están sujetas al criterio del Comité de IT y el tiempo de ejecución puede variar dependiendo de los recursos asignados a cada proyecto (Tipo A, Tipo B o Tipo C)
f. Se define a través de este procedimiento que se deben realizar los siguientes entregables a la Gerencia de Operaciones de IT, según el tipo de proyecto, previo pasó a producción de los sistemas de información

7.3.1. Metodología Aplicada

a. Proyectos tipo A: Se debe aplicar la metodología de proyectos del Planeación "MN-PI-003 Metodología para la Gestión de Proyectos de Servicios Postales Nacionales S.A."
b. Proyectos tipo B y tipo C: Se debe aplicar el procedimiento "PR-IT-009 Requerimientos de Sistemas de Información".

7.3.2. Entregables de Proyectos

a. Como parte del proceso de gestión de proyectos se deben tener como mínimo los siguientes entregables definidos como documentación del proyecto:
b. Levantamiento de requerimiento.
c. Estimación y aprobación de horas de ejecución del requerimiento.
d. Hitos de Entrega.
e. Pruebas de aceptación.
f. Registros/actas de Capacitación o socialización.
g. Solicitud de Control de Cambios y Publicaciones.

7.4. PASO A PRODUCCIÓN DE SISTEMAS DE INFORMACIÓN

7.4.1. Ambientes de un Sistema de Información

En Servicios Postales Nacionales S.A., deben existir tres ambientes en los sistemas de información que son:

- Desarrollo
- Pruebas
- Producción

Como lineamiento de la Dirección Nacional de Informática y Tecnología, se debe garantizar por parte de la Gerencia de Operaciones IT y las Gerencias de Proyectos IT, que los desarrollos y/o soluciones de información cumplan con los siguientes pasos:

- Desarrollo en ambientes exclusivos para este fin.
- Paso a ambiente exclusivo de pruebas, diferente al de desarrollo y producción en el cual se certifica que la aplicación cumple con los requisitos establecidos.
- Paso a producción liderado por el Administrador de Aplicaciones y BD.

7.4.2. Entrega de Proyectos de Sistemas de Información

Entregas Tipo A:

- Reunión de Entendimiento a las áreas de IT (Al inicio del proyecto)-Equipo de Operaciones IT
- Manual de Infraestructura (Si la solución tiene componentes de infraestructura) – Coordinador de Infraestructura
- Manual de la Aplicación (Si Aplica) - Administrador de Aplicaciones y BD
- Manual de Arquitectura (Si Aplica) - Administrador de Aplicaciones y BD
- Manual de Configuración (Si Aplica)-Administrador de Aplicaciones y BD
- Manuales de usuarios (Si Aplica)- Mesa de ayuda
- Acuerdos de Niveles de Servicio con proveedores (Si Aplica)- Administrador de Aplicaciones y BD
- Registros de Capacitaciones a usuarios finales y a funcionarios de IT-Mesa de ayuda Nivel 1 y Nivel 2
- Entrega de procedimiento de escalamientos hacia el proveedor (Si Aplica)- Administrador de Aplicaciones y BD
- Acta de Cierre -Carpeta de proyectos
- Acta de Cierre de Acompañamiento en Producción (3 meses)
- Soporte de pruebas y certificación – Carpeta de proyectos

Entregas Tipo B:

- Reunión de Entendimiento- Equipo de Operaciones IT
- Manuales técnicos (Si Aplica)
- Manuales de usuarios (Si Aplica)
- Manual de Arquitectura (Si Aplica)
- Registros de capacitaciones a los usuarios finales e IT
- Certificación de pruebas exitosas
- Acta de Cierre de Acompañamiento en Producción (2 meses)

Entregas Tipo C:

- Manuales técnicos (Si Aplica)
- Manuales de usuarios (Si Aplica)
- Registros de capacitaciones a los usuarios finales e IT
- Certificación de pruebas exitosas
- Acta de Cierre de Acompañamiento en Producción (15 días)

***Nota**: Para pasar al Comité de Cambios deben estar cumplidos los entregables en un 100%, excepto el acta de cierre de acompañamiento en producción.*

Operaciones IT será responsable de la funcionalidad o requerimiento puesto en producción una vez se encuentre estable y cumplidos los tiempos de acompañamiento (definidos en los entregables anteriormente mencionados) por parte de la Gerencia de Proyectos IT.

7.5. CONTROL DE UTILIZACIÓN DE SOFTWARE Y HARDWARE

Cuando se realicen los mantenimientos de los equipos por parte del equipo de IT revisará el software que se encuentra instalado, si encuentra algún software gratuito este será desinstalado del equipo de cómputo.

El control de la instalación del software y usos de licencias serán controlados automáticamente y en tiempo real con la herramienta Herramienta de Gestion de la mesa de ayuda IT Assets Management, que permite identificar, inventariar, monitorear y realizar mantenimiento de los activos tecnológicos de software y hardware.

El control de uso y legalidad de software utilizado en la red corporativa estará controlado en tiempo real con la herramienta Herramienta de Gestion de la mesa de ayuda IT Software Metrix.

Los equipos de la entidad se encuentran controlados por políticas de directorio activo que limitan los privilegios de instalación de software con un usuario estándar del equipo.

7.5.1. Disposición final de software y hardware

El hardware y software que sea clasificado como obsoleto después de evaluación de concepto técnico será retirado del inventario de IT y se entregara un diagnostico escrito con acta de devolución al almacén general de la entidad.

7.6. DOCUMENTACIÓN DE APLICACIONES

La documentación de los aplicativos administrados por Servicios Postales Nacionales S.A serán controlados por medio del formato "MN-IT-019-FR-003 Ficha Técnica de Aplicaciones".

8. CUMPLIMIENTO DE LA POLÍTICA

8.1. Cumplimiento de la Política de Seguridad

Cada dueño de proceso/subproceso de Servicios Postales Nacionales S.A., velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

La Dirección Nacional de Informática y Tecnología realizará revisiones aleatorias en las áreas de Servicios Postales Nacionales S.A a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Usuarios.

Los responsables de la información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

8.2. Sanciones por Incumplimiento de la Política

La Política de Seguridad es de obligatorio cumplimiento, por los colaboradores, consultores, contratistas, terceros.

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

Se sancionará administrativamente y disciplinariamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias que rigen al personal en el Reglamento Interno de Trabajo y en la Cláusula de Reserva de la Información en el Contrato Laboral, y en caso de corresponder, el

Proceso de Gestión Humana realizará las acciones correspondientes desde un llamado de atención hasta la terminación del contrato laboral.

9. IDENTIFICACIÓN DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	CRITERIO	CAMBIO
1	26/Jul/2016	Consideraciones Generales	Se incluyó una política en el numeral 1.1. Se modificaron los siguientes ítems: • 1.4 se incluyó el numeral 1.4.3. de Integrantes sobre la Gestión de Control de Cambios y Publicaciones. • 1.4 el rol de Coordinador de Aplicaciones por Administrador de Aplicaciones y BD Se incluyeron los siguientes ítems: • 1.5 Gestión de Proyectos • 1.6 Paso a Producción de Sistemas de Información • 1.8 Documentación de aplicaciones
2	Junio de 2018	Nombre del documento	Se integran el manual de informática y tecnología y el manual de políticas de seguridad de la información, y este se denomina **MANUAL DE INFORMÁTICA, TECNOLOGÍA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.**
2	Junio de 2018	Contenido	Se efectúan cambios en los siguientes literales: • Política de Clasificación y Control de Activos Informáticos • Política de Seguridad del Personal

			• Política de Seguridad Física y Ambiental • Política de Gestión de Comunicaciones y Operaciones • Política de Control de Acceso • Políticas de Utilización de Controles Criptográficos • Política de Gestión de Incidentes de Seguridad de la Información • Cumplimiento de la Política
3	Octubre de 2018	5.7. Logs de Auditorias 5.7.1. Administración de los Logs de Auditorias y sus responsables.	**5.7. Logs de Auditorias** **5.7.1. Administración de los Logs de Auditorias y sus responsables.** Se modifican los siguientes párrafos: …"es necesario e importante que el área de Control Interno Audite y Evalúe constantemente dichos logs, esto con el fin de prevenir cualquier circunstancia que pueda afectar la operación de la compañía. es necesario e importante también que el área de Operaciones y Gerencias Regionales monitoreen constantemente dichos logs, esto con el fin de prevenir cualquier circunstancia que pueda afectar la operación de la compañía" …