



I. OBJETIVO

La presente Política Operacional de TIC tiene por objetivo establecer las medidas y acciones que indican los puntos principales en el ámbito de tecnologías de la información y comunicación de la Secretaría Nacional de Deportes, determinando los responsables de las actividades, los documentos a ser utilizados, los niveles de autorización y la actualización de la presente política, a efectos de asegurar su vigencia y nivel de eficacia.

II. ALCANCE

- Los lineamientos que se detallan en el presente documento aplican a toda información de la Secretaría Nacional de Deportes que es implantada, recepcionada, almacenada, procesada, transmitida, entregada o eliminada, utilizando cualquier sistema informático o medio de almacenamiento (información digital).
- Diseño e implementación de los mecanismos apropiados (sistematizados o manuales) que permitan un acertado control sobre las tecnologías de la información y comunicación de la institución.
- Las políticas de seguridad de la Información se dictan en cumplimiento de normas actuales, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y los recursos tecnológicos de la Institución.
- Los accesos a la información, de forma segura, para los directivos y áreas en general de la institución.
- Los procedimientos para la correcta utilización y comprensión de los sistemas y recursos informáticos de la institución.
- Estas políticas son aplicables a todos los funcionarios, consultores, terceras partes, que usen las tecnologías de información y la comunicación de la institución.
- Esta política se encuentra alineada con las normas estándares internacionales como COBIT 5 y CIS Controls, para garantizar una gestión informática eficaz y segura.

III. RESPONSABLE DE APLICACIÓN:

- ▶ Direcciones Generales y Direcciones
- ▶ Dirección de Tecnologías de la Información y Comunicación

IV. DEFINICIONES:

- **Activo:** Cualquier cosa que tenga valor para la institución.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la institución.
- **Carácter Especial:** Son los símbolos que no son carácter numéricos ni del alfabeto, por ejemplo: (.;+*/=-_)
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Continuidad:** Capacidad de la Gestión de Servicios de Tecnología para continuar con la entrega de productos o servicios a los niveles predefinidos aceptables después de un evento perjudicial.
- **Desastre o contingencia:** Interrupción de la capacidad de acceso a información y procesamiento de la misma, por medio de equipos de cómputo u otros medios necesarios para la operación normal de un negocio.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Equipos Informáticos:** se entiende por equipos informáticos, a la PC de escritorio o notebook portátil, con sus componentes accesorios (monitor, teclado, mouse), teléfonos móviles, tablets o cualquier otro equipo que permita ingresar, procesar, almacenar, extraer o transmitir información. Quedan incluidos cualquier equipo periférico que pueda ser conectado a los equipos de computadoras: impresoras, scanners, proyectores, fotocopiadoras, módems, teléfonos móviles.
- **Políticas:** Toda intención y directriz expresada formalmente por la administración de la Organización.
- **Procesos:** Se define un proceso de negocio como conjunto de actividades que reciben una o más entradas para crear un resultado/producto de valor para el cliente o para la propia compañía/proceso (concepto



de Cliente Interno de Calidad). Normalmente, una actividad empresarial cuenta con múltiples procesos que sirven para el desarrollo su objeto de negocio.

- **Procedimientos:** Pasos operacionales que los colaboradores deben realizar para alcanzar ciertos objetivos/resultados.
- **Red:** conjunto de dispositivos que interconecta numerosas estaciones de trabajo, servidores y otros sistemas entre sí y hacia Internet.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Puede involucrar otras propiedades como autenticidad, trazabilidad (accountability), no repudio y fiabilidad.
- **TIC:** Se refiere a las Tecnologías de Información y Comunicación.
- **Vulnerabilidad:** Debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

V. DELINIAMIENTOS

1. POLÍTICAS GENERALES

1.1. La Secretaria Nacional de Deportes adopta como Política Operacional de TIC el de desarrollar una eficiente, eficaz, oportuna y correcta gestión de los servicios y recursos tecnológicos, cumpliendo con las normas y metodologías vigentes como COBIT 5, CIS Controls para el usufructo adecuado de los mismos.

1.2. La Secretaria Nacional de Deportes, establece los siguientes lineamientos:

- Hacer uso de la Política Operacional de TIC como parte de sus instrumentos de gestión y definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.
- Implantar y aplicar la política Operacional de TIC a todo el funcionario relevante, de forma que estén incorporadas y sean parte integral de las operaciones institucionales.
- El cumplimiento de la Política Operacional de Tecnologías de la Información y Comunicación (TIC) es obligatorio. Si los funcionarios, consultores, terceras partes violan estas políticas, la institución se reserva el derecho a tomar las medidas correspondientes.
- Las excepciones a cualquier cumplimiento de Política Operacional de TIC deben ser aprobadas por el Director de TIC, Director General de Gabinete y/o la Máxima Autoridad de la Institución. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas por los mismos.
- Las modificaciones o adiciones de la Política Operacional de TIC serán propuestas por la Dirección de TIC, validadas por el Director General de Gabinete y aprobadas por la Máxima Autoridad de la Institución. Esta política debe ser revisada como mínimo una vez al año o cuando sea necesario, para adaptarla a los cambiantes del entorno operativo.
- Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.
- A los usuarios se le brinda acceso a la red informática como instrumento para el desempeño de sus tareas. Todos los usuarios tienen la responsabilidad de utilizar los recursos informáticos de la institución de una manera ética, legal, óptima y profesional.
- Acogerá los criterios, normas y técnicas establecidas por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), entidad técnica e instancia rectora en el ámbito de las Tecnologías de la Información y Comunicación en el sector público, y de la comunicación del Poder Ejecutivo del Paraguay.

2. POLÍTICAS DE OPERACIÓN

2.1. Usufructo responsable de recursos



La Secretaria Nacional de Deportes podrá proporcionar una PC a cada usuario según la necesidad del cargo que ocupa, teniendo en cuenta lo autorizado por el Director de su dependencia.

- 2.1.1. Está prohibida la descarga, copia y ejecución de juegos, videos, innecesarios, a través de dispositivos externos, así como también la instalación de software (programas) que no estén autorizados.
- 2.1.2. Los usuarios son responsables de los archivos de uso personal almacenados en los recursos proporcionados por la institución.
- 2.1.3. El usuario debe apagar los equipos que tiene a su cargo, tales como la Unidad Central de Procesamiento (CPU), monitores e impresoras y desconectar la notebook de la red eléctrica una vez finalizada la jornada laboral.
- 2.1.4. El usuario responsable del equipo informático al que fue asignado, tiene prohibido realizar cambios en la configuración del mismo.
- 2.1.5. Está prohibido el retiro de los equipos informáticos de la institución sin la autorización de su jefe inmediato superior.
- 2.1.6. La Dirección de TIC, será la única encargada de instalar o desinstalar los programas que pueda necesitar cada equipo informático, así como el traslado, reparación o actualización.
- 2.1.7. La Dirección de TIC, a través de su Departamento de Soporte Técnico será la responsable de establecer un procedimiento para el mantenimiento de los equipos informáticos.
- 2.1.8. El mantenimiento de los equipos informáticos asignados a los usuarios deberá realizarse semestralmente, conforme al cronograma de mantenimiento respectivo.

2.2. Administración de la Red

La administración de recursos informáticos de la Red es responsabilidad de la Dirección de TIC de la Secretaria Nacional de Deportes, específicamente del Departamento de Infraestructura, será responsable de la administración de los Servidores de Internet, Bases de Datos propias de la institución, supervisión del tráfico de red, la seguridad de accesos a la red y servicios como: Dominios, servidores DHCP, los firewalls, proxys y/o la instalación de nuevos enlaces, hardware de conectividad tales como Hubs, Routers, módems o analizadores de protocolos.

El uso de las redes será monitoreado con el objetivo de ajustar y planificar la capacidad, de acuerdo con el desempeño requerido para cumplir con las funciones de cada usuario en la institución. Lo relacionado a Internet, el usuario tendrá acceso solamente a los sitios y páginas que le sean habilitadas y no sean consideradas como distractoras o perjudiciales para el horario laboral.

2.3. Correo electrónico

- 2.3.1. El uso del correo se encuentra condicionado a lo estrictamente laboral. De recibirse correos electrónicos que no correspondan al destinatario, el mismo debe ser eliminado y se debe comunicar la eliminación del correo electrónico al remitente.
- 2.3.2. Cada usuario es directamente responsable de todo lo enviado a través de sus cuentas de correo electrónico.
- 2.3.3. El usuario No deberá abrir los correos en los que exista duda de su procedencia y comunicara al Departamento de Soporte Técnico.
- 2.3.4. El espacio de almacenamiento disponible en el servidor de correo es limitado, motivo por el cual se recomienda que el usuario con cuenta de correo, consulte diariamente el webmail, lo descargue o administre conforme a la disponibilidad del espacio.
- 2.3.5. Es tarea de todo usuario de correo electrónico, la buena administración del espacio asignado a su cuenta de correo.
- 2.3.6. Se recomienda crear carpetas para la mejor administración del correo y mantener la bandeja de entrada con la menor cantidad de mensajes.
- 2.3.7. Se recomienda no mantener almacenados en el correo archivos que ocupen demasiado espacio. Si éstos son necesarios para el usuario deberá almacenarlos en su equipo de cómputo. El usuario será responsable del perjuicio que pueda ocasionar el no poder recibir o enviar más correos en caso de que se agote el espacio en el servidor.
- 2.3.8. Es obligación de cada usuario, mantener su recipiente de elementos eliminados, continuamente vacío, ya que esto representa espacio de correo utilizado innecesariamente, debido a que implica la saturación de la capacidad de almacenamiento del servidor.
- 2.3.9. El personal del Dpto. de Infraestructura, monitoreará las cuentas que presenten un comportamiento sospechoso para la seguridad de la información institucional, detección de intrusos, propagación de virus, seguridad de la red de la SND e inclusive podrá ir al lugar del usuario a verificar en su PC el uso que le esté dando a su correo institucional.



2.3.10. Los usuarios de la SND, no podrán hacer envíos de mensajes masivos de correo electrónico, salvo las cuentas autorizadas por la máxima autoridad. Los mensajes masivos no deberán ni podrán ser enviados desde una cuenta de correo gratuito (Hotmail, Gmail, etc.) ya que esto pone en riesgo el servicio al ser la institución emisora catalogada Spammer (creadora de correo basura) y posteriormente incluida dentro de las "listas negras" empleadas para el bloqueo del dominio completo por otros servidores de correo.

2.4. Seguridad

Cada usuario es responsable de la información contenida en el equipo a su cargo y por lo tanto debe resguardarla.

2.4.1. Inventario de dispositivos y software autorizados y no autorizados

Se debe gestionar activamente todo dispositivo hardware y software en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso.

Hardware

- Utilizar una herramienta de descubrimiento activo para identificar equipos conectados a la red de la organización y actualizar el inventario de activos hardware.
- Utilizar una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la organización y actualizar automáticamente el inventario de activos.
- Mantener un inventario veraz y actualizado de todos los activos tecnológicos capaces de almacenar y/o procesar información. El inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.
- Asegurar que el inventario de activos de hardware registre, como mínimo, las direcciones de red, nombre, propósito, responsable, departamento de cada activo, así como también si el activo de hardware ha sido aprobado o no para ser conectado a la red.
- Asegurar de que los activos no autorizados se eliminen de la red, se pongan en cuarentena o el inventario se actualice oportunamente.

Software

- Mantener una lista actualizada de todo el software autorizado que es requerido en la organización para todos los fines de negocio y todos los sistemas de negocio.
- Asegurar que en el inventario de software autorizado de la organización se incluya únicamente software (aplicaciones o sistemas operativos) que actualmente cuente con soporte del fabricante. El software que no cuenta con soporte debe ser marcado como no soportado en el sistema de inventario.
- El sistema de inventario de software debe obtener el nombre, la versión, el autor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la organización.
- El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado sean rastreados desde una sola ubicación.
- Asegurar que el software no autorizado es removido, o que sea incluido en el inventario oportunamente.

2.4.2. Protección contra software maliciosos

Se deben implementar controles de detección, prevención, recuperación y concientización, con el fin de que los usuarios tengan protección frente a software maliciosos.

Todos los equipos informáticos deben contar con antivirus instalados y activos, periódicamente deben ejecutarse procesos de búsquedas de virus en los equipos.



2.4.3. Seguridad en las redes

Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y para mantener la seguridad de los sistemas y aplicaciones.

Se deben implantar controles relacionados con la segmentación, gestión, monitoreo y detección de eventos, para asegurar la información que viaja por las redes.

2.4.4. Registros de Auditoría

Se deben conservar registros de auditoría de las actividades de los usuarios, incluyendo administradores y operadores, de las excepciones o incidentes de información y mantenerlos durante un período acordado para ayudar en investigaciones futuras y en el seguimiento y monitoreo del control de acceso:

En la medida de lo posible se incluirá como mínimo en los registros:

- Identificadores de usuarios.
- Registro de intentos de acceso al sistema exitosos y rechazados.
- Registro de intentos de acceso a los recursos y a los datos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de dispositivos y aplicaciones del sistema.
- Archivos a lo que se ha accedido y la clase de acceso.
- Alarmas por el sistema de control de acceso.
- Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión.
- Cambios o intentos de cambios en las posiciones y en los controles de seguridad del sistema.

2.4.5. Gestión de usuarios y contraseñas

Todos los usuarios que acceden a recursos informáticos de la Red requieren de una única e intransferible identidad o login (nombre de usuario) para una persona. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la Red.

La Dirección de TIC, proporcionará este identificador como parte del proceso de autorización. Los identificadores concedidos son dados de baja cuando la Dirección de Talento Humano solicita procesar la baja correspondiente a dicho identificador de usuario por desvinculación del funcionario de la institución.

El usuario y password asignado a un funcionario es personal e intransferible, cada usuario es responsable de los servicios y recursos que le sean asignados bajo esas credenciales.

Características de las contraseñas

- La contraseña debe tener una longitud mínima de 8 caracteres.
- La contraseña debe contener letras mayúsculas, minúsculas y números, es decir deben ser alfanuméricos e indefectiblemente contener al menos 1 (una) letra mayúscula en el primer carácter, y contener un carácter especial.
- Las contraseñas tienen un periodo de validez de 180 días, forzando al usuario a cambiarla al cumplirse ese término.

2.4.6. Copias de Respaldo

Las copias de seguridad de la información y de software se deben realizar periódicamente, considerando lo siguiente:

Back Up de Equipos Informáticos de la Institución, el Dpto. de Soporte Técnico deberá realizar las copias de respaldo de cada estación de trabajo de la Secretaría Nacional de Deportes según lo establecido en los procedimientos establecidos para ello, semestralmente.



2.5. Carpetas Compartidas

Los administradores de la red establecen e implementan en los casos aprobados la configuración de acceso a las carpetas, previo requerimiento formal del Superior Inmediato.

El usuario que autoriza el acceso a las carpetas y dispone el recurso compartido, es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

Se debe definir el tipo de acceso y los roles estrictamente necesario sobre la carpeta (lectura, escritura, modificación, borrado). Además, se debe especificar el límite de tiempo durante el cual estará publicada la información y el recurso compartido en el equipo.

Para la información confidencial o crítica para la compañía, deben utilizarse las carpetas destinadas en el servidor de archivos de usuarios, con el fin de que sea incluida en las copias diarias de respaldo.

El acceso a carpetas compartidas debe delimitarse a los usuarios que realmente necesitan la información y se debe proteger el ingreso con contraseñas.

No se puede compartir carpetas o el acceso a carpetas compartidas, a usuarios que no cuenten con software de antivirus corporativo y actualizado.

2.6. Adquisición e Implementación de Sistemas

El Departamento de Infraestructura dependiente de la Dirección de TIC, es la responsable de la adquisición, implementación y actualización de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), asegurar la calidad de los servicios entregados y de acuerdo con criterios de innovación, confiabilidad, disponibilidad, seguridad, economía e interoperabilidad, que den soporte a la productividad de los colaboradores en los procesos.

Cuando un área requiera implementar un software, plataforma tecnológica o sistemas de información, debe diligenciar el respectivo formato de requerimientos y asignar a una persona responsable para liderar la implementación solicitada.

Para el manejo y administración de los requerimientos tecnológicos (adquisiciones, implementación y actualización), el Departamento de Infraestructura tiene la responsabilidad de hacer las pruebas necesarias.

La propiedad intelectual de los desarrollos contratados será propiedad de la Institución, salvo acuerdo escrito expreso que diga lo contrario.

El proceso de adquisición y desarrollo de las aplicaciones debe ser estructurado y ordenado, considerando las diferentes etapas del ciclo de vida de las soluciones.

La documentación de cada uno de los sistemas implantados en la institución debe contener la guía para brindar soporte a los usuarios.

2.7. Gestión de incidentes

Todos los incidentes ocurridos en ámbitos de TIC en la institución deben ser registrados, clasificados, actualizados, escalados, resueltos y cerrados.

La gestión de incidentes debe ser supervisada y revisada. Se deben realizar informes de los problemas gestionados.

2.8. Gestión de Continuidad


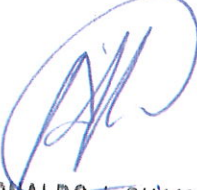
Se deben identificar los requisitos de continuidad para los servicios en función de las necesidades de la institución.

Los requisitos se registran en un Plan de continuidad, el cual será revisado por lo menos una vez al año y siempre que se produzcan cambios significativos. Una vez realizados los cambios se debe



probar el plan para comprobar su adecuación y documentar el resultado de las pruebas. En caso que no se alcancen los resultados previstos, se deben establecer acciones encaminadas a su consecución.

*** **

Elaborado por:	Revisado por:	Aprobado por:
 Lic. Roberto Bogarín Dirección de Informática TIC's SECRETARIA NACIONAL DE DEPORTES PRESIDENCIA DE LA REPUBLICA	 MG. ARNALDO J. CHAMORRO DIRECTOR GENERAL DE GABINETE SECRETARIA NACIONAL DE DEPORTES PRESIDENCIA DE LA REPUBLICA	 Rolando Coronel Comité de Control Interno
Cargo: PRESIDENCIA DE LA REPUBLICA Fecha de elaboración:	Cargo: SECRETARIA NACIONAL DE DEPORTES PRESIDENCIA DE LA REPUBLICA	Cargo: Presidente Secretaria Nacional de Deportes