MINISTERIO de EDUCACIÓN CIENCIA y TECNOLOGÍA PRESIDENCIA de la NACIÓN

Instituto Nacional de Educación Tecnológica

Perfil Profesional
Sector Informática

Técnico Superior en Soporte de Infraestructura de Tecnología de la Información

Perfil Profesional
Técnico Superior en Soporte de Infraestructura de Tecnología de la Información

Ámbito de Desempeño

Los sistemas informatizados son desarrollados por grupos multidisciplinarios organizados por proyecto y sobre especificaciones elaboradas a partir de un análisis de problemas a resolver, los que en muchos casos son los informativos y operativos que tienen las organizaciones.

Los sistemas comprenden el software que realice las funciones previstas, incluyendo interfaces con usuarios, archivos de datos que exploten esos programas y los procedimientos correspondientes. Su funcionamiento requiere de una infraestructura tecnológica apropiada. Esto significa disponer de estaciones de trabajo para los usuarios, de servidores ubicados en la organización o fuera de ella que alojen a aplicaciones, datos, eventualmente otros sistemas con los cuales deban comunicarse, redes locales o de área extendida que los vinculen y el software de base necesario para que funcione todo, es decir, sistemas operativos, sistemas para administración de redes, sistemas de bases de datos.

Por regla general, las estaciones de trabajo de los usuarios constituyen la parte más simple y que administra el propio usuario, recurriendo en caso de necesidad al apoyo de una mesa de ayuda o de técnicos de soporte al usuario (en Informática Profesional y Personal).

Salvo el software del sistema en sí, que es soportado por el área de sistemas o de desarrollo de software, del resto de la infraestructura, excepto la rutina operativa, se ocupan Administradores de Sistemas o Administradores de Redes, que son técnicos que se ocupan del soporte y administración de servidores, sistemas de almacenamiento, software de base, subsistemas y redes de comunicación de datos. Según la dimensión y características de la organización, se desempeña un único técnico que se ocupa de todo, incluyendo aspectos de seguridad y deriva problemas que lo exceden a profesionales o servicios externos especializados, o varios técnicos, cada uno de los cuales suele especializarse en un tipo de tecnología o en partes determinadas de la instalación.

La administración y soporte del resto de la infraestructura tecnológica suele tener carácter crítico ya que por lo general las aplicaciones requieren prestar servicios ininterrumpidamente, bajo exigencias de seguridad y confiabilidad, con tiempos de respuesta predecibles, por lo cual el principal objetivo de estos técnicos es maximizar el tiempo durante el cual los sistemas estén en condiciones de prestar esos servicios, eventualmente diagnosticando y resolviendo los inconvenientes que puedan impedirlo.

Perfil Profesional

El Técnico Superior en Soporte de Infraestructura de Tecnología de la Información estará capacitado para implementar, mantener, actualizar, analizar inconvenientes y resolver problemas derivados de la operación de productos de tecnología de la

información que cumplen funciones de sistema operativo, administración de almacenamiento, comunicaciones y redes, seguridad, bases de datos, y otros subsistemas, para garantizar la máxima disponibilidad del ambiente operativo de las aplicaciones informáticas de las organizaciones desarrollando las actividades descriptas en el perfil profesional y cumpliendo con los criterios de realización establecidos para las mismas, para lo cual coordinará o complementará su trabajo con especialistas de la misma organización o externos.

Áreas de Actividad

1. Administrar servidores, software de base, comunicaciones y demás subsistemas, optimizando el aprovechamiento de los recursos y anticipando posibles problemas.

2. Administrar redes de comunicación de datos asegurando la accesibilidad de los servicios y optimizando los recursos.

3. Atender incidentes que afecten a la infraestructura de tecnología de información, diagnosticar las causas que los originan y resolverlos o coordinar su solución.

4. Instalar o reemplazar componentes de la infraestructura de tecnología de la información o adaptarla a nuevas condiciones de servicios externos, minimizando riesgos para la seguridad y continuidad del servicio.

5. Migrar o convertir sistemas, aplicaciones o datos tratando de minimizar riesgos para la seguridad y continuidad del servicio.

6. Entender en temas de contingencias y riesgos que puedan afectar a la infraestructura de tecnología de la información.

El trabajo competente del técnico en estas áreas de actividad requiere no sólo de poseer conocimientos específicos de las tecnologías involucradas, sino del desarrollo de una competencia para diagnosticar las situaciones o problemas que tenga que afrontar, la que resulta crítica para su desempeño porque facilita el discernimiento entre causas y efectos para resolver los problemas que afecten a la disponibilidad de los recursos.

Complementariamente a esto, es importante que el técnico adquiera una actitud de servicio que privilegie el interés colectivo organizacional a las conveniencias individuales y técnicas, ya que de su labor dependerá el trabajo de muchos usuarios de los sistemas de aplicación.

Capacidades Transversales

a. Abstracción
Implica descartar o reducir detalles poco significativos de la información sobre un objeto o situación tanto para simplificarlos y concentrarse en pocos elementos por vez, lo que reduce su complejidad y facilita su comprensión, como para generalizarlos y conceptualizarlos a fin de poder relacionarlos con otros modelos, problemas o soluciones conocidas, facilitando el diagnóstico de situaciones y el análisis de posibles soluciones.

b. Razonamiento inferencial
Implica actuar metódicamente para asociar características de incidentes con posibles causas de mal comportamientos, así como propiedades de productos y rendimientos observados o acciones previas y resultados obtenidos, para elaborar diagnósticos de situaciones y descartar acciones ineficaces para su solución.

c. Anticipación
Implica anticiparse a los hechos, adoptar una actitud proactiva analizando indicadores y previendo su evolución o posibles problemas. También planificar las acciones a realizar, evaluando posibles alternativas con sus ventajas o desventajas, previendo y contrastando resultados, y capitalizando experiencias.

d. Asegurar la corrección
Implica controlar experimentalmente la integridad y corrección de sus acciones utilizando procedimientos sistemáticos de verificación de los resultados obtenidos que permitan corregir eventuales acciones con efectos no deseados.

e. Trabajar en equipo
Implica adoptar una actitud abierta, estar dispuesto a compartir información y conocimientos, o acordar objetivos, límites y pautas comunes con otros técnicos o especialistas de la misma organización o de otras colaborando para resolver los problemas presentados. También implica preocuparse por hacer comprensibles y documentar adecuadamente las decisiones tomadas.

f. Comunicarse apropiadamente
Supone reconocer su rol y el de cada integrante de la organización, transmitir la información necesaria en forma precisa y en un lenguaje apropiado para el entendimiento mutuo en interacciones individuales o grupales, o en forma escrita, utilizando, si es necesario para ello, el idioma inglés, que debe interpretar con propiedad a nivel técnico.

f. Autoaprendizaje
Implica aprender a capitalizar experiencias a partir de su propio trabajo, a tomar iniciativas para actualizar o profundizar sus conocimientos y habilidades, investigar fuentes de información o herramientas que le pueden resultar útiles. Aplica metodologías de investigación y dedica tiempo a este fin.

Desarrollo del Perfil Profesional

1. Administrar servidores, software de base, comunicaciones y demás subsistemas, maximizando el aprovechamiento de los recursos y anticipando posibles problemas.	
Función o Actividad	**Criterios de realización**
1.1. **Monitorear** la distribución de carga del sistema y los recursos que componen la Infraestructura.	• Se emplean los instrumentos adecuados. • Se anticipan eventuales problemas. Se mantiene una comunicación adecuada con los responsables involucrados.

1.2. **Asignar**, **liberar** y **reorganizar** espacios de almacenamiento en medios magnéticos.	• La distribución de carga evoluciona de acuerdo con los márgenes planificados.
1.3. **Otorgar**, **modificar** o **cancelar** permisos a usuarios de sistemas y subsistemas.	• El sistema permanece protegido dentro de las políticas de seguridad.
1.4. **Actualizar**, **implementar** cambios o **aplicar** parches en software de base, configurando lo que corresponda.	• Se mantiene actualizado el registro de los cambios realizados. • En función de su interacción con otros equipos o software, se reconfiguran otros componentes que lo requieran
1.5. **Requerir** a proveedores externos cambios en sus instalaciones o servicios.	• Se coordinan acciones para minimizar interrupciones del servicio. • Se verifica o testea lo que los proveedores realizan. • Se exige la actualización de la documentación que corresponda.
1.6. **Administrar** backups.	• Se acuerdan las frecuencias y modalidades con cada responsable. Se automatizan los procedimientos pasibles de ser programados. • Se administran los archivos de disponibilidad inmediata. • Se prevé un entorno de pruebas y se realizan éstas para verificar la efectividad del recupero.
1.7. **Automatizar** operaciones rutinarias o previsibles para ganar eficiencia y seguridad en la operación.	• Se programan comandos para ejecutar tareas rutinarias o cuya buena ejecución puede resultar crítica. • Se prevén posibles errores y se incluyen acciones alternativas en los scripts o programas.
1.8. **Analizar** logs y herramientas de medición para verificar la eficiencia del sistema y la utilización de los recursos de la infraestructura de IT.	• Se observan y señalan situaciones o tendencias proponiendo acciones de mejora.
1.9. **Planificar** la capacidad para anticipar situaciones y proponer soluciones que mantengan la eficiencia y efectividad del sistema.	• Se realiza un análisis periódico de los resultados de los diversos monitoreos para extraer conclusiones. • Se anticipan saturaciones de recursos. Se optimiza la utilización de recursos, balaceando su disponibilidad. • Se proponen soluciones: – compatibles con la arquitectura de las plataformas, o – nuevas que ofrezca el mercado, y que – - consideren aspectos económicos.

2. Administrar redes de comunicación de datos asegurando la accesibilidad de los servicios y optimizando los recursos	
Función o Actividad	**Criterios de realización**
2.1. **Configurar** switches y routers de acuerdo a estándares definidos.	• Las configuraciones responden a los requisitos. • Se documentan las configuraciones. • Se prevén backups para respaldo de las configuraciones.

2.2. **Monitorear** el tráfico reasignando recursos y reconfigurando ruteos para balancear la carga.	• Se identifican cuellos de botella. Se alerta con anticipación sobre eventuales comportamientos anómalos. El tráfico y utilización de los recursos evoluciona de acuerdo con los márgenes planificados.
2.3. **Mantener** el parque electrónico de la red.	• Se actualiza en tiempo y forma el microcódigo de switches y routers. Se verifican vínculos de backup.
2.4. **Mantener** el cableado estructurado de acuerdo a las normativas existentes.	• Se documentan las conexiones, incluyendo las interracks e interpatch. Se verifica el estado integral de toda la instalación. • Se coordinan acciones con proveedores o instaladores del cableado estructurado.
2.5. **Anticipar** situaciones y **proponer** soluciones que mantengan la eficiencia y efectividad del sistema.	• Se realizan monitoreos periódicos y analiza el impacto del crecimiento (usuarios y recursos). • Se anticipan congestiones de tráfico. • Se proponen soluciones para la conectividad y configuración de dispositivos.

3. Atender incidentes que afecten a la Infraestructura de TI, diagnosticar las causas que los originan y resolverlos o coordinar su solución	
Función o Actividad	**Criterios de realización**
3.1. **Identificar** el problema que dio lugar al incidente	• Se descartan metódica y rápidamente causas alternativas fuera de su responsabilidad.
3.2. **Establecer** prioridades para su solución, tomando en cuenta las posibles consecuencias del problema para la operatoria de la organización.	• Se realiza un análisis de riesgos evaluando el impacto del problema en las actividades de la organización. • Se proponen soluciones que consideran operatorias críticas para la organización y minimizan su *downtime*.
3.3. **Investigar** y **diagnosticar** el origen o causa última del problema para generar una solución duradera.	• Se utilizan logs y otros instrumentos de monitoreo que aporten elementos de juicio al diagnóstico. • Se profundiza en por qué se produjeron las condiciones que posibilitaron el incidente.
3.4. **Planificar** las acciones necesarias para resolver el problema.	• Se prevén acciones complementarias y se estiman tiempos para minimizar el lapso total.
3.5. **Derivar** a otros integrantes del equipo o a terceros la solución o acciones necesarias para la misma.	• Se recurre a quienes poseen el know how más adecuado para encarar cada parte de la solución prevista. • Se les aporta la información necesaria para que puedan realizar su labor.
3.6. **Realizar** las acciones necesarias y coordinarlas con las que tienen que realizar otros integrantes del equipo o terceros.	• Se actúa de acuerdo a estándares de procedimiento. • Se contemplan riesgos para la operatoria adoptando los recaudos debidos. • Se trabaja en equipo con propios y ajenos proporcionando la información necesaria. • Se controla la eficacia y eficiencia de servicios provistos por terceros comparando con acuerdos de nivel de servicio.

3.7. **Verificar** mediante pruebas que la solución implementada haya resuelto el problema.	• Se considera no sólo el funcionamiento de lo modificado sino también la interacción de ese componente con otros de la infraestructura TI.
3.8. **Administrar** el problema y documentar lo actuado	• Se inician partes de incidentes y se va documentando lo actuado hasta llegar a la solución o la transferencia del problema a otro responsable. • Se actualizan los backups de las configuraciones modificadas.

4. Instalar o reemplazar componentes de la Infraestructura de TI o adaptarla a nuevas condiciones de servicios externos minimizando riesgos para la seguridad y continuidad del servicio	
Función o Actividad	**Criterios de realización**
4.1. **Informarse** sobre las características técnicas de nuevo software o hardware a instalar o las nuevas condiciones técnicas del servicio y analizar el efecto de su incorporación sobre otros componentes de la plataforma y la eficiencia del sistema.	• Se muestra solvencia técnica sobre las características y operación del componente. • Se muestra comprensión técnica de las nuevas condiciones del servicio. • Se opta por la decisión más apropiada considerando posibles efectos.
4.2. **Planificar** las actividades necesarias para la instalación, incluyendo el resguardo de datos o versiones anteriores de software, su eventual recuperación y la verificación del buen funcionamiento conjunto del componente instalado.	• Se considera realizar la instalación en un entorno de testing antes de su implementación efectiva. • Se consideran problemas técnicos. • Se consideran eventuales riesgos para las operaciones y datos de la organización, adoptando las previsiones necesarias.
4.3. **Avisar** a la gerencia o usuarios involucrados sobre las consecuencias previstas para la operabilidad del sistema.	• Se aconsejan acciones que minimicen sus posibles inconvenientes. • Se toman en cuenta las actividades de cada destinatario y adapta la información.
4.4. **Instalar** versiones de prueba de software de base en un entorno de prueba / laboratorio, configurando lo que corresponda y testeando su operabilidad y comportamiento	• Se consideran necesidades de reconfigurar redes u otro software a raíz de esta instalación o de las nuevas condiciones de servicios externos. • Se verifica su interoperabilidad con otros componentes bajo condiciones de seguridad. • Se mide el comportamiento del nuevo software o, de ser posible, se hace una prueba piloto del servicio.
4.5. **Reemplazar** componentes de hardware que se puedan cambiar en forma directa.	• Se consideran problemas de compatibilidad y riesgos.
4.6. **Preparar** backups de los componentes modificados para poderlos reponer rápidamente en caso de necesidad.	• Se contemplan posibles partes interesadas (desarrolladores, proveedores) y se acuerda con ellos qué resguardar.

	• Se contempla e incluye todo lo necesario para poner en funcionamiento el componente. • Se resguardan archivos de configuración.
4.7. **Preparar** y **mantener** actualizada documentación sobre el *layout* físico y lógico de las distintas plataformas y la Infraestructura de TI.	• Se incluyen todos las componentes y sus vinculaciones, planteando eventualmente niveles de detalle. • Se identifica clara y unívocamente cada componente. • Se incluyen referencias a documentación complementaria necesaria.

5. Migrar o convertir sistemas, aplicaciones o datos tratando de minimizar riesgos para la seguridad y continuidad del servicio	
Función o Actividad	**Criterios de realización**
5.1. **Analizar** las características propias de la nueva tecnología y capacitarse para operar en forma segura sobre la misma y aprovecharla debidamente.	• Se toma en cuenta el software o aplicación a migrar y su posible impacto sobre otro software o las comunicaciones del sistema.
5.2. **Analizar** todo lo que requiere instalarse, resguardarse, modificarse, trasladarse y recuperarse o poner en marcha y testear para planificar o intervenir en la planificación de las tareas a realizar.	• Se toman en cuenta los archivos o bases con datos a ser procesados por el nuevo software y el impacto del nuevo formato que tengan esos datos sobre otro software que los utilice. • Se toman en cuenta riesgos de perder o afectar datos u operaciones en el proceso de migración. • Se planifica el rollback de lo implementado en caso de comportamientos técnicos no deseados. Se toman en cuenta niveles de actividad y criticidad de la operatoria involucrada para establecer la oportunidad en que se realizara efectivamente la migración.
5.3. **Prever** contingencias y realizar ensayos o pruebas piloto para asegurarse que lo planificado es adecuado.	• Se prevén inconvenientes o pérdidas durante la migración y se resguardan los datos o sistemas que corresponda Se realizan tests previos para asegurarse que la migración ha sido correcta.
5.4. **Acordar** con la gerencia y usuarios fechas y condiciones de corte y reanudación para que organicen sus propias actividades.	• Se propone y acuerda con antelación y con quien corresponda (la gerencia, los usuarios) la oportunidad del corte de la operatoria y se les suministran instrucciones precisas que minimicen posibles inconvenientes.
5.5. **Coordinar** con otros involucrados las tareas del plan de migración.	• Se incorporan márgenes razonables a lo planificado para manejar imprevistos.
5.6. **Realizar** las acciones necesarias	• Se actúa de acuerdo a estándares de procedimiento. • Se trabaja en equipo con propios y ajenos proporcionando la información necesaria y revisando los procedimientos y resultados.
5.7. **Verificar** el adecuado funcionamiento del sistema migrado antes de liberarlo a sus usuarios.	• Se acuerda un protocolo de pruebas con el área de sistemas y usuarios.

	• Se realizan pruebas parciales o totales para asegurarse que la migración ha sido exitosa a su nivel de responsabilidad.

6. Entender en temas de contingencias y riesgos que puedan afectar a la Infraestructura de TI.	
Función o Actividad	**Criterios de realización**
6.1. **Evaluar** riesgos que puedan afectar a la continuidad del funcionamiento del sistema.	• Se distingue entre riesgos provenientes de agentes internos o externos, de infraestructura física o lógica, derivados de contingencias en proveedores, riesgos que afectan operaciones críticas para la organización. • Se proponen medidas para contrarrestar esos riesgos o resolver situaciones de contingencia.
6.2. **Intervenir** en la confección de planes de contingencia.	• Se documenta el plan, incluyendo aspectos esenciales de los sistemas, diagramas topológicos, gráficos de conexión y datos involucrados. • No se omiten aspectos esenciales.
6.3. **Verificar** mediante pruebas que los planes de contingencia y acciones de recuperación se mantengan válidos.	• Se configura un entorno de testing para realizar las pruebas. • Se realizan periódicamente pruebas y simulaciones que permitan verificar que los procedimientos de emergencia y de recuperación son efectivos. • Se documentan y analizan los resultados obtenidos, capitalizando experiencias y proponiendo mejoras.
6.4. **Implementar** medidas de seguridad lógicas y físicas respecto a riesgos externos.	• Se actualizan listas negras y blancas de acuerdo a políticas establecidas. • Se mantienen listas de formas de contacto para atender contingencias con ISPs y otros proveedores de servicios críticos. • Se mantienen listas de DNS confiables alternativos.
6.5. **Implementar** medidas de seguridad contra riesgos internos o que simulan serlo.	• Se asignan los recursos en función de la política de seguridad establecida. • Se establecen y asignan perfiles en función de la política y procedimientos de seguridad establecidos, controlando periódicamente su validez. • Se mantiene la seguridad de los VPN. Se inhibe la instalación de software no autorizado de acuerdo a políticas de la organización. • Se establecen y controlan condiciones de renovación de contraseñas en función de políticas de la organización. • Se controla periódicamente la validez de certificaciones de accesos web en función de políticas de la organización. • Se prueban periódicamente procedimientos de lucha contra principios de incendio y eventual evacuación del data center.
6.6. **Interviene** en temas de seguridad perimetral.	• Se alerta sobre eventuales riesgos. Se cumple y se hace cumplir los procedimientos relativos al acceso físico a las instalaciones.

Campo y condiciones del ejercicio profesional

Principales resultados del trabajo
Una infraestructura de tecnología de la información que se encuentra disponible y cumple su función en forma ininterrumpida o con un mínimo aceptable de inconvenientes, facilitando la operación de las aplicaciones que operan sobre la misma.
Soluciones a eventos o situaciones que afecten a la disponibilidad, capacidad, rendimiento o seguridad de la infraestructura y que tengan una eficacia y eficiencia compatibles con las condiciones y políticas organizativas.
Advertencia temprana y sugerencias sobre cómo afrontar posibles saturaciones de recursos u otros riesgos referidos tanto a la capacidad como a la seguridad.

Medios de producción o de tratamiento de la información
Servidores y clusters, locales o remotos; dispositivos de almacenamiento; otros dispositivos de hardware; sistemas operativos, máquinas virtuales y administradores de redes; servicios comunicaciones a través de redes públicas o privadas; dispositivos de switching; firewalls; motores de bases de datos; subsistemas como servidores de e-mail, de impresión, etc. Utilitarios, herramientas de diagnóstico, lenguajes de scripting.

Procesos, técnicas y regulaciones normativas
Hojas de especificaciones, instructivos de procedimientos, manuales con información técnica y ayudas en línea sobre los objetos de su trabajo.
Normas ITIL, ISO, CCITT e IEEE. Normas aplicables a las comunicaciones digitales.
Normas legales –propiedad del software y de los datos comerciales o industriales de una empresa, protección de datos personales–, políticas y disposiciones propias de la organización y normas de auditoría que regulan a los servicios de TI.

Datos e información disponibles o generados
Internet, correo electrónico, foros y listas de discusión.
Genera informes sobre trabajo realizado y reportes de incidentes.

Espacio social de trabajo: relaciones funcionales o jerárquicas
Este técnico se desempeña en centros de procesamiento de datos, ya sean de empresas usuarias de tecnología de la información o empresas que brindan servicios a éstas sin que obligatoriamente deba estar físicamente ubicado en los mismos.
Por lo general, depende directa o indirectamente de un Gerente de Tecnología responsable por toda la operación y, en función de la dimensión de la organización en la cual se desempeñe, puede trabajar solo, en pequeños grupos o en grupos más grandes que permitan su especialización en determinadas tecnologías.
Intercambia información, colabora con sus pares u otros especialistas propios o externos en la solución de los problemas observados.
En la mayoría de los casos no tiene personal a cargo.

Proceso de Consulta

Análisis Ocupacional

Recomendaciones del Plan Estratégico 2004-2014 del Foro de la Competitividad para el Sector de Software y Servicios Informáticos organizado por la Secretaría de Industria, con participación de la CEPYME, Ministerios de Educación, Ciencia y Tecnología, de

Trabajo, Empleo y Desarrollo Social y de Relaciones Exteriores, como también de representantes de entidades, organizaciones, empresas y universidades.

Reuniones de definición y seguimiento realizadas por un Grupo de Trabajo compuesto por representantes de CESSI, Cámara de Empresas de Tecnología, de CICOMRA, Cámara de Informática y Comunicaciones de la República Argentina, del Polo IT Buenos Aires, de SADIO, Asociación Argentina de Informática, a los que se agregaron intercambios de información con el Polo Tecnológico de Rosario, el Polo IT de La Plata (en formación) y ATICMA (de Mar del Plata).

Visitas y entrevistas a Empresarios, Líderes de Equipo y Técnicos de las siguientes organizaciones:

- Sistemas Activos S.A.
- Acriter S.A.
- Calipso S.A.
- IBM Global Delivery Services
- Caja de Valores S.A.
- Banco Credicoop
- ATS S.A.

así como aportes personales de profesionales de nuestro país y del exterior.

Consulta de material estadístico relativo al empleo en el sector, entre el cual se encuentra el informe sobre Situación y Perspectivas del Capital Humano TICC en Argentina y de referencia sobre perfiles profesionales.

Taller de Reflexión realizado el 26 y 27/10/2008 sobre las actividades que desarrolla un técnico recopilados o realizados con la colaboración de las siguientes organizaciones:

- IBM Global Delivery Services
- Banco Credicoop
- Secretaría de Hacienda de la Nación
- Caja de Valores S.A.

Validación del Perfil Profesional

El Perfil fue revisado y validado por el mismo Grupo de Trabajo que participó de su definición y seguimiento. También fue difundido a quienes participaron de talleres o realizaron aportes, así como expertos del campo.