CAMINOS Y PUENTES FEDERALES DE INGRESOS Y SERVICIOS CONEXOS

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

CAPUFE

CAMINOS Y PUENTES FEDERALES

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

NOVIEMBRE 2024

SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ÍNDICE

I. INTRODUCCIÓN

El presente documento se establece en apego al *"ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal".*

…

"CAPÍTULO VI

SEGURIDAD DE LA INFORMACIÓN

…

Artículo 75.- *Las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de SI, que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, a través de sus sistemas, aplicaciones, infraestructura y personal; dicho MGSI deberá contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.*

La política general de seguridad de la información está orientada a garantizar certidumbre en la continuidad de la operación y la permanencia e integridad de la información institucional".

Mismo que tiene por objeto dictar lineamientos de observancia obligatoria en la Administración Pública Federal. Esta Política forma parte de la base para establecer el Marco de Gestión de Seguridad de la Información (MGSI) en Caminos y Puentes Federales de Ingresos y Servicios Conexos (CAPUFE), con el fin de proteger los datos y activos de información que soportan su operación, reducir los riesgos por el uso de las Tecnologías de la Información y Comunicaciones (TIC), así como para conformar el Modelo de Gobierno de Seguridad de la Información en CAPUFE.

La persona Titular de la Subdirección de Tecnologías de la Información, responsable de la Seguridad de la Información (RSI) de CAPUFE, en ejercicio de sus facultades conferidas, tiene a bien definir los

controles de seguridad necesarios para salvaguardar los Activos de TIC, Infraestructuras críticas, así como a los Activos de información del organismo, motivo por el que se expide el presente documento.

II. OBJETIVO GENERAL

Establecer la base normativa que soporte la implementación del Marco de Gestión de Seguridad de la Información para contribuir al cumplimiento de leyes y regulaciones aplicables en materia de seguridad de la información, reducir los riesgos e impactos operativos, financieros, de imagen, de reputación, fortalecer la eficacia y eficiencia de los procesos de CAPUFE.

III. OBJETIVOS ESPECÍFICOS

1. Establecer los criterios y directrices generales sobre la seguridad de la información, aplicables a CAPUFE.

2. Fortalecer la cultura de prevención de riesgos de seguridad de la información por medio de la sensibilización.

3. Orientar las acciones sobre la gestión de seguridad de la Información, a fin de que estén alineadas con los objetivos institucionales de CAPUFE.

4. Garantizar la seguridad de la información y minimizar los riesgos, a través de un impacto provocado por una gestión eficaz de la misma.

5. Garantizar la disponibilidad requerida, de los sistemas informáticos críticos para el desarrollo de los procesos del Organismo.

IV. FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.
  D.O.F. 05/02/1917 y sus últimas reformas.

- Ley Federal de Transparencia y Acceso a la Información Pública.
  D.O.F. 09/05/2016 y sus últimas reformas.

- Ley General de Responsabilidades Administrativas.
  D.O.F. 18/07/2016 y sus últimas reformas.

- Ley General de Transparencia y Acceso a la Información Pública.
  D.O.F. 04/05/2015 y sus últimas reformas.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
  D.O.F. 26/01/2017.

- Ley General de Archivos.
  D.O.F. 15/06/2018 y sus últimas reformas.

- Ley Orgánica de la Administración Pública Federal.
  D.O.F. 03/01/1977 y sus últimas reformas.

- Código Penal Federal.
  D.O.F. 14/08/1931 y sus últimas reformas.

- ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024.
  D.O.F. 06/09/2021.

- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.
  D.O.F. 06/09/2021.

- Lineamientos para la Emisión y Actualización de Normas Internas de CAPUFE.
  Fecha de publicación en la Normateca Interna: 11/09/2023.

- Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

- Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos.
  D.O.F. 30/04/2021 y su última modificación.

- Código de Conducta de CAPUFE. Vigente.

- NMX-I-27001-NYCE-2015.
  D.O.F. 14/04/2015 y sus últimas reformas.

- ISO/IEC 27001:2013.
  D.O.F. 14/04/2015 y sus últimas reformas.

V. ÁMBITO DE APLICACIÓN

Las políticas contenidas en este documento, aplican para todo el personal que labore o preste servicios a CAPUFE, así como a la gestión, operación, información y activos de información que soportan los procesos sustantivos y adjetivos de CAPUFE.

VI. DEFINICIONES

- **Amenaza:** Cualquier posible acto que pueda causar algún tipo de daño a los activos de información de CAPUFE.

- **CAPUFE y/u Organismo:** Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- **Centro de Datos:** Sala o instalación física que alberga la infraestructura de TI para crear, ejecutar y entregar aplicaciones y servicios. También almacena y gestiona los datos asociados con esas aplicaciones y servicios.

- **Compilador:** Programa de cómputo que traduce un programa escrito en un lenguaje de programación a lenguaje máquina.

- **Confidencialidad:** La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

- **Contraseña:** Conjunto de caracteres utilizados para acceder a información reservada en un sistema, servicio, sitio web, computador o a un dispositivo móvil.

- **Control:** Mecanismo automatizado o manual utilizado para proteger los datos y activos de información, garantizando su confidencialidad, integridad y disponibilidad.

- **Disponibilidad:** La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

- **Dueño de la Información:** Persona Servidora Pública de CAPUFE con nivel mínimo de Gerencia, responsable de implementar y operar los controles que garantizan la confidencialidad, integridad y disponibilidad de la información a su cargo.

- **Dueño del Activo de Información:** Persona Servidora Pública de CAPUFE con nivel mínimo de Gerencia, responsable de implementar y operar los controles que garantizan la confidencialidad, integridad y disponibilidad de los activos de información a su cargo.

- **ERISC:** Equipo de respuesta a incidentes de seguridad en TIC en CAPUFE.

- **Externo:** Persona física o moral que presta algún servicio contractual a CAPUFE y que hace uso de información y/o cuenta con acceso a tecnologías de información y telecomunicaciones propiedad de CAPUFE.

- **GESI:** Grupo estratégico de seguridad de la información. Integrado por personas servidoras públicas que conozcan los procesos institucionales y que cuenten con conocimientos en materia de seguridad de la información, mediante el documento de integración y operación del grupo estratégico de seguridad de la información.

- **GTDTIC:** Grupo de trabajo para la dirección de TIC, integrado por personas servidoras públicas con nivel mínimo de Dirección de Área.

- **Información:** Conjunto de datos que soportan el funcionamiento, procesos y toma de decisiones.

- **Integridad:** La acción de mantener la exactitud y corrección de la información y sus métodos de proceso y de la infraestructura tecnológica.

- **ISO/IEC 27001:2013:** ISO 27001, Estándar internacional sobre los requerimientos de sistemas de gestión de seguridad de la información.

- **Mesa de Ayuda:** Herramienta de software o un equipo de agentes humanos que le permite a una empresa brindar soporte a sus clientes en tiempo real.

- **MGSI:** El Marco de Gestión de Seguridad de la Información que, por medio del análisis de riesgos y de la definición de procesos y controles, define las guías para establecer, implementar, mantener, mejorar, monitorear, operar y revisar la seguridad de la información.

- **NMX-I-27001-NYCE-2015:** Norma mexicana sobre los requerimientos de sistemas de gestión de seguridad de la información.

- **OICE:** Órgano Interno de Control Específico.

- **Persona Usuaria:** Persona que emplea un producto o servicio, bien de forma ocasional, bien de forma habitual.

- **Persona Trabajadora:** Persona física que presta a otra, física o moral, un trabajo personal subordinado.

- **Riesgo:** La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de CAPUFE.

- **Script:** Bloque de instrucciones del sistema operativo de la computadora, que se ejecutan secuencialmente para completar una tarea.

- **Seguridad de la Información:** La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la responsabilidad, autenticidad, confiabilidad y trazabilidad.

- **Software:** Instrucciones, rutinas y programas elaborados en lenguajes de programación, para realizar una tarea específica.

- **STI:** Subdirección de Tecnologías de la Información.

- **TIC:** Las tecnologías de información y comunicaciones que comprenden el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video.

- **Validación:** La actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

- **Verificación:** La actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

- **Vulnerabilidad:** La debilidad en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de información y a la infraestructura crítica.

VII. DISPOSICIONES GENERALES

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información y activos de información que soportan los procesos sustantivos y adjetivos de CAPUFE deben estar protegidos, garantizando la confidencialidad, integridad y disponibilidad de la información institucional, para satisfacer las expectativas de nuestros clientes, asociados, entidades regulatorias y demás partes interesadas; así como para el logro de los objetivos y estrategias de CAPUFE.

Para dar cumplimiento a lo anterior, se debe operar bajo un Marco de Gestión de Seguridad de la Información, alineado a las políticas y disposiciones de la Coordinación de Estrategia Digital Nacional, y que cumpla con los requerimientos establecidos en el estándar nacional NMX-I-27001-NYCE-2015 y en el estándar internacional ISO/IEC 27001:2013, promoviendo actividades de mejora continua, administración de riesgos y mejora regulatoria para asegurar la continuidad operacional y reducir impactos adversos a CAPUFE por el uso de información y las tecnologías de la información y comunicaciones (TIC).

Es responsabilidad de todas las personas servidoras públicas de CAPUFE y externos, en el ámbito de su competencia, cumplir con esta política para proteger la información que utilizada en la operación del día a día.

1.1. Directrices Generales

La Política de Seguridad de la Información debe ser publicada y comunicada a las personas servidoras públicas de CAPUFE y externos.

Para gestionar los objetivos de seguridad de la información, se debe designar a una persona Responsable de la Seguridad de la Información (RSI).

La Política de Seguridad de la Información debe estar enfocada a los temas específicos que exigen la aplicación de los diversos controles de seguridad de la información:

a) Protección de datos personales
b) Cumplimiento de leyes y regulaciones
c) Control de acceso a la información
d) Desarrollo de sistemas

La Política de Seguridad de la Información se encuentra alineada al Marco de Gestión de Seguridad de la Información de la Coordinación de Estrategia Digital Nacional, atendiendo a los requerimientos de:

a) Continuidad Operativa del Negocio.
b) Legislación, reglamentos, contratos y demás normatividad aplicable.
c) El entorno actual y futuro de amenazas de seguridad de la información.

1.2. La o el Dueño de la Política

La o el dueño de la Política de Seguridad de la Información es la persona Responsable de la Seguridad de la Información (RSI) que será designada por la persona Titular de la Dirección General de CAPUFE. El RSI, tendrá entre otras, las siguientes responsabilidades:

I. Dar seguimiento a la conformación del MGSI, así como a su implementación y al cumplimiento de los controles mínimos de seguridad;

II. Presentar a sus superiores jerárquicos, incluido el Titular de la Institución, un informe sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución. En la presentación deberá considerarse la presencia de la persona Titular de la STI cuando el rol de RSI no recaiga en éste;

III. Dar aviso inmediato a la CEDN sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;

IV. Implementar un programa de evaluaciones, que contemple al menos, una evaluación trimestral del MGSI para verificar el desempeño de los controles de seguridad y determinar acciones de mejora;

V. Hacer del conocimiento del OICE en la institución y/o de las autoridades competentes, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia; así como

VI. Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.

1.3. Incumplimiento

Es responsabilidad de todas las personas servidoras públicas de CAPUFE, notificar al Responsable de Seguridad de la Información, cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

El incumplimiento de las disposiciones de la Política de Seguridad de la Información, será(n) sancionado(s) de conformidad a su gravedad, a efecto de que se determinen las responsabilidades que procedan en términos de los ordenamientos legales aplicables, el RSI deberá hacer del conocimiento del OICE en CAPUFE, y cuando corresponda, de las autoridades que resulten competentes, del incumplimiento a la Política de Seguridad de la Información.

La aplicación de esta Política es de carácter obligatorio, la revisión de su cumplimiento podrá realizarse bajo auditorías programadas anualmente, auditorías de seguimiento, revisiones particulares o cualquier otro medio autorizado. Las revisiones serán realizadas por el RSI y el ERISC; así como por el Órgano Interno de Control Específico, dependencias y entidades federales y/o consultores externos.

1.4. Homologación y Estandarización

La supervisión de la implementación de los controles de seguridad para proteger la información y activos de información, estarán a cargo de la Subdirección de Tecnologías de la Información y deben estar homologados evitando la existencia de varios controles aplicables para un mismo fin; deben estar enfocados a la efectividad y eficiencia en el uso de recursos (humanos, financieros y tecnológicos), y en la medida de lo posible deben estar automatizados evitando el uso de controles manuales.

2. POLÍTICAS ESPECÍFICAS

2.1. Protección de la Información

La seguridad de la información es responsabilidad de todas las personas usuarias de CAPUFE. Cada persona usuaria deberá realizar las acciones necesarias para proteger la seguridad de la información, de manera enunciativa mas no limitativa:

1. Bloquear el equipo cuando se ausente del lugar asignado.
2. Recoger de las impresoras los documentos con información crítica o sensible.
3. El escritorio o pantalla del equipo no debe tener accesos o archivos con información crítica o sensible, en la medida de lo posible no debe tener accesos o archivos de uso interno.

2.2. Control de Accesos a Equipos y Servicios TIC

1. Todos los accesos a los equipos informáticos son restringidos a personal ajeno, salvo que sea autorizado por la persona Titular de la Gerencia de Infraestructura de Tecnologías de Información.

2. Todos los equipos que accedan a la red inalámbrica de CAPUFE, se deberán registrar en los servicios de red por parte de la Subgerencia de Telecomunicaciones.

3. La Subdirección de Tecnologías de la Información, a través de la Gerencia de Atención a Usuarios de Tecnologías de Información y la Gerencia de Infraestructura de Tecnologías de Información, establecerá los mecanismos de autenticación para el acceso a redes de la organización como validación por dominio o persona usuaria y/o contraseña.

4. La Subdirección de Tecnologías de la Información, a través de la Gerencia de Atención a Usuarios de Tecnologías de Información y la Gerencia de Infraestructura de Tecnologías de Información, deberá retirar los accesos de personal que dejen de laborar en el Organismo. Por lo que la Subdirección de Capital Humano y Desarrollo Organizacional, deberá informar cuando menos 24 horas antes de la baja para que se realicen las acciones necesarias para retirar los permisos a la infraestructura, programas y sistemas en materia informática.

5. La Subdirección de Tecnologías de la Información, a través de la Gerencia de Atención a Usuarios de Tecnologías de Información y la Gerencia de Infraestructura de Tecnologías de Información, deberá revisar y modificar los accesos al menos cada 6 meses, después de cambios mayores o cuando se produzca un incidente de seguridad.

6. El acceso a los videos de las cámaras de vigilancia de Oficinas Centrales y Órgano Interno de Control Específico, sólo puede ser autorizado por la persona Titular Subdirección de Tecnologías de la Información o la persona Titular de la Gerencia de Infraestructura de Tecnologías de Información.

2.2.1. Acceso a la Red Institucional

1. Para redes inalámbricas se deberá realizar la petición por cada persona usuaria a través de formato libre, en donde justifique el acceso a este tipo de redes:
    - La o el solicitante necesariamente deberá ser persona trabajadora del Organismo.
    - Para hacer uso de este servicio, se deben de registrar las personas usuarias que deseen la prestación del servicio, vía Mesa de Ayuda y presentando el dispositivo que se conectará a la red inalámbrica.

- Se debe registrar la dirección MAC de las tarjetas inalámbricas de todos y cada uno de los dispositivos institucionales de comunicación.

2. La Subdirección de Tecnologías de la Información, a través de la Gerencia de Infraestructura de Tecnologías de Información, deberá controlar el acceso a redes internas al personal interno y externo mediante medidas de aseguramiento de las contraseñas y demás mecanismos de conexión.

2.2.2. Responsabilidad de la Persona Usuaria en el Uso de Contraseñas o Información Secreta de Autenticación

1. No compartir contraseñas.
2. No guardar las contraseñas en lugares fácilmente identificables.
3. Mantener secreta la información de autenticación.
4. Cambiar la información secreta de autenticación siempre que exista un indicio de riesgo o se cumpla la vigencia de la misma.

2.3. Uso de Correo Electrónico Institucional

1. Las cuentas de correo electrónico generadas son de carácter personal e intransferible.
2. Es deber de cada persona usuaria asegurarse de cerrar la sesión de trabajo una vez que finalice la utilización del servicio de correo electrónico correspondiente, con el fin de que nadie más pueda utilizar su identificación.
3. Para el envío de correos electrónicos donde el contenido sea de uso exclusivo del Organismo, deberá efectuarse haciendo uso de un correo electrónico institucional.
4. Queda prohibido el uso del correo electrónico para contextos diferentes al ámbito diferente a la función de CAPUFE, dentro y hacia afuera de la Institución.
5. Queda prohibido enviar información sensible, por correo electrónico, cuentas FTP, o cualquier, medio electrónico. Es decir, información considerada como *clasificada, confidencial o que, sin*

serlo, el usuario no tenga atribuciones que permitan su uso y divulgación. Asimismo, que prohibido atentar contra los derechos de autor, enviar información falsa, difamatoria u ofensiva.

6. La generación de cuentas y su correspondiente clave de acceso, será mediante solicitud expresa del Titular del Área interesada, dirigida a la Subdirección de Tecnologías de la Información.
7. En caso de que la persona usuaria olvide su cuenta de correo electrónico y/o su contraseña, deberá solicitarla nuevamente en forma personal a la Mesa de Ayuda en la extensión 3999.
8. Las cuentas de correo electrónico serán eliminadas a solicitud expresa de las personas Titulares de las Áreas, o de acuerdo al cambio de estatus laboral de las personas usuarias.

2.4. Uso de Internet

1. La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todas las personas usuarias tienen las mismas responsabilidades en cuanto al uso de Internet.
2. El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
3. No está permitido acceder a Internet llamando directamente a un proveedor (a) de servicio.
4. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.
5. El uso de Internet considerado inaceptable puede comprender la pérdida del acceso, dar lugar a la revocación de permisos sobre Internet, una investigación administrativa y/o las sanciones legales aplicables. Se considera uso inaceptable del servicio de Internet los siguientes:
    - Descargar material con expresa y manifiesta propiedad intelectual u otros derechos necesarios para dicha descarga o uso, sin los permisos necesarios, las licencias que correspondan o cualquier otro formalismo que deba cumplirse y se omita intencionalmente.
    - Para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, sonidos u obras que puedan infringir el marco normativo vigente referido a propiedad intelectual, marcas o patentes.

- Al involucrarse o participar de cualquier manera en actividades ilícitas en cualquier sitio y desde cualquier dispositivo conectado a la red desde el servicio de Internet.
- Para la divulgación de información deliberadamente falsa, sensible o difamatoria sobre personas o instituciones en cualquier sitio o herramienta disponible en línea (correo electrónico, webs, wiki, redes sociales, chat, foros, etc.).
- Sin contar con herramientas básicas de resguardo y seguridad, instaladas en el computador o dispositivo a emplear, a saber: antimalware y las actualizaciones del sistema operativo que posea el computador o dispositivo. La validación de estas condiciones será determinada y puede consultarse en el área técnica.
- Hacer uso de herramientas de software instaladas que habiliten servicios potencialmente riesgosos para CAPUFE.
- En situaciones que afecten la dignidad humana, tengan carácter discriminatorio u ofensivo, sean usados para amenazar y generar persecuciones a personas o empresas, generen situaciones de acoso laboral, sexual, contrarias a la moral, pornografía o similares.
- El uso de programas para compartir archivos (Peer to Peer).
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- Uso de JUEGOS "on line" en la red.

2.4.1. Integración de Dispositivos a la Red Informática de CAPUFE

Persona Usuaria Externa

1. Las personas servidoras públicas, mandos medios y superiores, que autorizan el acceso a la persona usuaria externa a las instalaciones de CAPUFE, deberán solicitar al Titular de la Subdirección de Tecnologías de la Información, por medio de correo electrónico o documento formal el levantamiento de una petición de servicio (ticket) en la Mesa de Ayuda de TI, para el acceso del o los dispositivos de la persona usuaria externa a la red informática de CAPUFE, acompañándolo del o los formatos de solicitud de servicios (Ver ANEXO) y documentación correspondientes:
    - Formato de solicitud proveedor.

- Reglas de Operación del Uso del Servicio de Internet.
- Acuerdo de confidencialidad y no divulgación proveedor.
- Formato de solicitud de cuenta de acceso VPN proveedor.
- Reglas de operación del servicio de VPN.
- Copia de una identificación oficial vigente con fotografía (credencial de elector, pasaporte o cédula profesional) de la persona usuaria externa.

2. El personal de la Mesa de Ayuda de TI, deberá validar que el dispositivo a incorporar a la red informática, cuente con antivirus actualizado (de aplicar) e interfaz de conexión a la red de datos (alámbrica o inalámbrica).

3. El personal de la Mesa de Ayuda de TI, deberá registrar el nombre de la persona usuaria externa, la dirección física (MAC-Address), asignar dirección IP y realizar la configuración de red en el dispositivo de la persona usuaria externa a los servidores de acceso de CAPUFE.

4. El personal de la Mesa de Ayuda de TI, en conjunto con la persona usuaria externa, deberán validar la correcta conexión del equipo.

5. El personal de la Mesa de Ayuda de TI, deberá asignar los permisos de Internet solicitados (en caso de haberse requerido).

6. El personal de la Mesa de Ayuda de TI, en conjunto con la persona usuaria externa, deberá verificar que el equipo tenga el acceso a Internet solicitado.

7. El personal de la Mesa de Ayuda de TI, deberá documentar en herramienta de Mesa de Ayuda de TI, la atención brindada a la petición de servicio (notas a ticket).

8. El personal de la Mesa de Ayuda de TI, deberá adjuntar evidencia de la atención a la petición de servicio y realizar el cierre del mismo, notificando de forma automática vía correo electrónico a la persona servidora pública solicitante.

2.4.2. Acceso a los Servicios de la Red Informática

Persona Usuaria Interna

1. La persona usuaria interna de CAPUFE, deberá levantar la petición de servicio (Ticket) en la Mesa de Ayuda de TI, vía telefónica a la ext. 3999, para solicitar el acceso a los servicios de la red informática.

2. El personal de la Mesa de Ayuda de TI, deberá evaluar los requerimientos solicitados de la persona usuaria interna de CAPUFE, para asesorarla a requisitar el o los formatos de solicitud de servicios (Ver ANEXO) correspondientes:

    - Formato de solicitud internet.
    - Reglas de Operación del Uso del Servicio de Internet.
    - Acuerdo de confidencialidad y no divulgación CAPUFE.
    - Formato de solicitud de cuenta de acceso VPN.
    - Reglas de operación del servicio de VPN.

3. La persona usuaria interna de CAPUFE, deberá entregar al personal de la Mesa de Ayuda de TI, el o los formatos de solicitud de servicio requisitados, firmados y validados.

4. El personal de la Mesa de Ayuda de TI, deberá realizar la asignación de servicios de la red informática de CAPUFE.

2.4.3. Asignación de los Servicios de Internet

a) Las personas con nivel de mandos medios y superiores serán las únicas personas servidoras públicas autorizadas para aprobar los niveles de los servicios de Internet, conforme a la siguiente tabla:

NIVELES PARA EL USO DEL SERVICIO DE INTERNET	
PUESTO	**NIVEL DE ACCESO**
Titulares de la Dirección General, Direcciones de Área, Coordinaciones, Secretaría Técnica, del Órgano Interno de Control Específico y Titulares de Área	NIVEL-5
Titulares de Unidades Regionales, Titulares de Subdirecciones de Área	NIVEL-4
Titulares de Gerencias, Titulares de Subgerencias	NIVEL-3
Personal Operativo	NIVEL-2
Proveedores	NIVEL-1
Personas Usuarias Internas que por su comportamiento pongan en riesgo equipos, información o se vea afectado el desempeño del servicio de Internet	NIVEL-0

Tabla 1 Personal autorizado para uso del servicio de internet por nivel jerárquico

b) Para la autorización de los accesos a la red informática de CAPUFE, se deberá llevar un control de las solicitudes mediante el formato "Solicitud de Alta, Baja o Cambio de Cuentas de Acceso para Personas Usuarias de Servicios de Tecnologías de Información", a través de las Gerencias de Infraestructura de Tecnologías de Información y la Gerencia de Atención a Usuarios de Tecnologías de Información, observando los siguientes requisitos:

1. Las solicitudes para acceso a Internet de acuerdo a los grupos "Nivel-1", "Nivel-2" y "Nivel-3", serán autorizadas por Titulares de las Subdirecciones de Área, Titulares de Unidades Regionales y Titulares de Área.
2. Las solicitudes para acceso a Internet de acuerdo a los grupos "Nivel-4" y "Nivel-5", serán autorizadas por Titulares de las Direcciones de Área, Titulares de Unidades Regionales y Titular del Órgano Interno de Control Específico.
3. La STI se reserva el derecho de asignar los permisos del grupo "Nivel-0" a la persona usuaria que por su comportamiento pongan en riesgo equipos, información o se vea afectado el desempeño del servicio de Internet, haciéndose del conocimiento de la persona Titular del Área correspondiente.

c) Con la finalidad de evitar accesos no autorizados a Internet que pongan en riesgo la seguridad de la red de datos del Organismo, en caso de que la persona servidora pública cambie de área de adscripción o cause baja, deberá notificar esta situación a la extensión 3999 para realizar los cambios necesarios en los permisos del uso del servicio de Internet.

d) La Subdirección de Capital Humano y Desarrollo Organizacional informará a la STI, los movimientos de altas, bajas y cambios del personal del Organismo, así como los cambios de adscripción, a fin de mantener actualizado el control de personas usuarias del servicio de Internet.

La STI se reserva el derecho de permitir o denegar el acceso a páginas o aplicaciones específicas a través de Internet, de acuerdo a las condiciones de utilización y seguridad del servicio de Internet, con la finalidad de evitar accesos no autorizados que pongan en riesgo la seguridad de la red de voz y datos del Organismo.

2.4.4 Descripción de Niveles de URL de los Servicios de Internet

A continuación, se describen los niveles de acceso a los servicios de INTERNET:

DESCRIPCIÓN DE NIVELES DE ACCESO	
NIVEL DE ACCESO	**DESCRIPCIÓN**
NIVEL-0 (SITIOS OFICIALES)	Solo se permite el acceso a páginas de gobierno, bancos y socios de negocio (ID México, lAVE).
NIVEL-1 (BÁSICO)	Acceso a categorías del Nivel-0 y sitios comerciales .COM como buscadores, sitios de educación, empresas.
NIVEL-2 (WEB-MAIL)	Cuenta con los permisos del Nivel-1, además de acceso a correo externo como Hotmail, Gmail, Yahoo! Mail.
NIVEL-3 (IM)	Cuenta con los permisos del Nivel-2, así como acceso a mensajería instantánea como, Google, WhatsApp, Telegram.
NIVEL-4 (SOCIAL NETWORK)	Cuenta con los permisos del Nivel-3, además de acceso a la red social oficial de CAPUFE Twitter, canales de noticias.
NIVEL-5 (STREAMING)	Cuenta con los permisos del Nivel-4, así como consulta de audio y video online como YouTube, estaciones de radio y Aplicativos de transferencia en la nube.

Tabla 2 Niveles de URL's

2.5. Respaldo de la Información

1. Toda la información de los procesos, proyectos, servicios y clientes (as) deberá estar respaldada. Es muy importante puntualizar que si bien, la Subdirección de Tecnologías de la Información es la encargada de realizar respaldos de los sistemas de información y bases de datos de uso común, es la persona usuaria, la directamente responsable de llevar a cabo los respaldos de la información que maneje.

2. Cada área o persona usuaria será responsable del respaldo de la información que generen.

3. Por lo que, para los sistemas designados de respaldo de información, toda la información contenida en el repositorio deberá ser considerada como oficial.

2.6 Transferencia de Información

2.6.1 Transferencia de Información a Proveedores o Clientes

1. En la medida de lo posible, evitar el envío de información sensible o crítica a personal externo al Organismo.

2. Hacer uso de las políticas de correo electrónico descritas en este documento.

2.6.2 Transferencia de Información Digital o Electrónica

1. Entregar de manera personal la transferencia de información sensible o crítica, validando la autorización e identidad de la persona que recibirá la información.

2. Transferencia de información utilizando mecanismos de autenticación y protocolos de cifrado o seguros previa autorización.

3. Proporcionar la información secreta de autenticación preferentemente de manera personal o como último recurso vía telefónica, no dejar esa información en contestadoras telefónicas ni buzones.

2.7. Solicitud de Personas Usuarias para Acceder a los Servicios TIC

La finalidad de la presente es para mitigar riesgos en la Seguridad Informática, en los accesos a los servicios e infraestructura tecnológica de CAPUFE, por lo tanto, se realiza el presente documento de las acciones que se deberán realizar, lo anterior para contar con los niveles de seguridad de permisos y accesos del personal activo y del personal que deja de laborar en el Organismo; a fin de darlos de baja de inmediato. En razón de lo anterior se deberán llevar a cabo las siguientes actividades por las áreas involucradas.

1. Todas las solicitudes de altas, bajas o modificación a los servicios e infraestructura Tecnológica de CAPUFE, deben realizarse por medio de oficio a la Subdirección de Tecnologías de la Información.

2. Las solicitudes de altas, bajas o modificación de datos de otras personas usuarias deben ser realizadas por la persona Titular del Área (al menos nivel Gerencia) pudiendo ser realizado por Subdirección o Dirección.

3. Las solicitudes de corrección de datos (nombre, apellido, persona usuaria, número de empleado (a) y/o correo electrónico) pueden ser realizadas por la persona usuaria, mediante ticket a la Mesa de Ayuda, en la extensión 3999 o 3666.

4. El escrito específico para BAJA DE PERSONA USUARIA deberá venir validado por la Subdirección de Capital Humano y Desarrollo Organizacional y la fecha en la que causará baja la persona trabajadora, este documento deberá de entregarse cuando menos 2 días hábiles previos a la baja cuando sean programables, y el mismo día de la baja cuando no lo sean.

5. Las personas usuarias invitadas, no tendrán acceso a la Red Institucional ni a ningún recurso de uso privado de CAPUFE.

2.7.1. Solicitud de Alta de Persona Usuaria

La solicitud de la debe incluir:

- Nombre completo de la persona usuaria.
- Número de empleado (a).
- Área de adscripción.
- Puesto que ocupará.

En caso de requerirse solicitud de permisos especiales de Acceso al SIAC, deberá de atender los formatos establecidos, para esta plataforma.

2.7.2. Solicitud de Baja de Persona Usuaria

La solicitud de la debe incluir:

- Nombre completo de la persona usuaria.
- Número de empleado (a).
- Área de adscripción.
- Puesto que ocupaba.

2.7.3. Solicitud de Modificación de Persona Usuaria

La solicitud de la debe incluir:

- Nombre completo de la persona usuaria.
- Número de empleado (a).
- Área de adscripción.
- Puesto que ocupa.
- Detalle claro y preciso de la modificación solicitada.

2.8. Solicitud de Acceso a Grabaciones y/o Tomas del Tipo Fotográfico del Sistema de Video - Vigilancia

El presente, documenta las acciones para atender las diferentes solicitudes de acceso a las videograbaciones y/o tomas del tipo fotográfico al Sistema de Video - vigilancia instalado en las Oficinas Centrales y Órgano Interno de Control Específico de CAPUFE. Con el fin de atender con eficiencia y eficacia las funciones que tiene encomendadas la Dirección de Administración y Finanzas, a través de la Subdirección de Tecnologías de la Información para la canalización y atención de incidentes detectados a través de las cámaras de Video - vigilancia y estandarizar la metodología de atención.

2.8.1. Videograbación

1. La STI deberá resguardar las videograbaciones por un periodo de al menos 15 días atrás.

2. El sistema para acceso a las videograbaciones, deberá estar resguardados con usuario y contraseña.

3. El personal administrador del sistema deberá estar adscrito a la Subdirección de Tecnologías de la Información.

4. Los accesos adicionales deberán ser solicitados de manera escrita a la Dirección de Administración y Finanzas y la persona Titular de ésta, será la única facultada para autorizar.

2.8.2. Solicitud de Tomas del Tipo Fotográfico

Es importante mencionar que la solicitud a los sistemas debe estar encaminada a la seguridad institucional y asuntos oficiales.

1. Se deberá llenar el "FORMATO DE SOLICITUD DE TOMAS DEL TIPO FOTOGRÁFICO" (Anexo 1 de la presente Política), expresando de manera clara la justificación.

2. La solicitud deberá estar validada por la persona Titular del Área (al menos nivel Gerencia) pudiendo ser realizado por la Subdirección o Dirección.

2.9. Acceso al Personal Visitante o Externo al Centro de Datos

1. La Subdirección de Tecnologías de la Información verificará y aprobará, a través de la Gerencia de Atención a Usuarios de Tecnologías de Información y/o la Gerencia de Infraestructura de Tecnologías de Información la solicitud de entrada y salida de equipo de proveedores (as) o personal externo autorizado para el ingreso a las instalaciones de la persona visitante.

2. La Subdirección de Tecnologías de la Información otorgará el acceso siempre y cuando se tenga autorización interna para la visita, a través de la Gerencia de Atención a Usuarios de Tecnologías de Información y/o la Gerencia de Infraestructura de Tecnologías de Información.

3. Para toda visita externa al Centro de datos de Oficinas Centrales de CAPUFE, se supervisarán las actividades a realizarse en los sistemas previa autorización de la Subdirección de Tecnologías de la Información.

4. Verificar que el personal externo porte un gafete que lo identifique como visitante durante su estancia en las instalaciones, así como corroborar la identidad de la persona.

5. No se permitirá a los proveedores (as) hacer uso de equipo tecnológico de grabación o video dentro de las instalaciones críticas sin una autorización previa.

2.9.1. Acceso a la Información por Personal Externo

1. Firma de un convenio de confidencialidad y/o acuerdo de transferencia de la información por parte del proveedor.

2. Cumplir con las medidas y protocolos de seguridad técnicas para la transferencia de la información.

3. Retirar el acceso otorgado cuando la seguridad de la información se vea comprometida o al finalizar el periodo autorizado.

2.9.2. Uso de los Recursos de la Organización

Para el personal visitante deberá apegarse a las siguientes políticas:

1. No dañar física o lógicamente los equipos o la infraestructura informática.

2. No tomar fotografías o video sin previa autorización.

3. No utilizar los recursos de CAPUFE sin previa autorización.

4. Evitar la descarga de programas, fotos, música, videos que no estén justificados durante su visita.

5. No conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización de la Subdirección de Tecnologías de la Información.

6. No instalar dispositivos de comunicaciones en los equipos e infraestructura tecnológica sin previo consentimiento Subdirección de Tecnologías de la Información a través de la Gerencia de

Atención a Usuarios de Tecnologías de Información y/o la Gerencia de Infraestructura de Tecnologías de Información.

7. No realizar acciones o actividades que incumplan las leyes o regulaciones de seguridad de la información.

2.10. Uso y Mantenimiento de Equipos y Sistemas de Tecnologías de Información

1. Se debe contar con autorización por escrito de la Subdirección de Tecnologías de la Información para el ingreso, uso y conexión a la red institucional de cualquier equipo de tecnología en instalaciones de CAPUFE.

2. Se debe contar con autorización por escrito de la Subdirección de Tecnologías de la Información para realizar cualquier trabajo de mantenimiento a la infraestructura tecnológica de CAPUFE:
   - Para el diseño de nuevas áreas o en el crecimiento de las áreas existentes, se deberán considerar los estándares vigentes de cableado estructurado. Por lo que en las Oficinas Centrales y el Órgano Interno de Control Específico se deberá coordinar con la Subdirección de Tecnologías de la Información y en Unidades Regionales con las Subgerencias de Administración.
   - Sólo será soportado el protocolo TCP/IPV.4 e IPV.6 en la red inalámbrica.

3. No se permite la operación ni instalación de "puntos de acceso" (access points) conectados a la red cableada sin la debida autorización por parte la Subdirección de Tecnologías de la Información.

4. No se permite configurar las tarjetas inalámbricas como "puntos de acceso" o la configuración de equipos como servidores adicionales.

5. No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.

6. Con la finalidad de evitar responsabilidades, en caso de que alguna persona usuaria haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar a la Mesa de Ayuda para su respectiva baja del equipo de la red inalámbrica.

7. En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos dos días hábiles.

2.11. Políticas para el Borrado Seguro de Información

Procedimiento de Borrado para Equipos de Arrendamiento:

1. Aplica cuando se va entregar el equipo de forma definitiva al proveedor.

2. Por medio de una memoria tipo USB Booteable con configuración para arranque de sistema operativo, eliminar particiones para dejar el equipo sin sistema operativo. De esta forma aseguramos la eliminación del licenciamiento.

Procedimiento de Borrado para Equipos Propios:

1. Aplica cuando se va entregar el equipo de forma definitiva al área de Bienes para Desecho, Obsolescencia.

2. Por medio de una memoria tipo USB Booteable con configuración para arranque de sistema operativo, eliminar particiones para dejar el equipo sin sistema operativo. De esta forma aseguramos la eliminación del licenciamiento.

Procedimiento de Borrado para Equipos de Arrendamiento/Propio Cuando se Reasignan:

1. Seleccionar y eliminar los perfiles de usuario que tenga el equipo.

2. Buscar y eliminar información que se encuentre en raíz (C o D).

3. Se crea los nuevos perfiles.

ANEXO 1

FORMATO DE SOLICITUD DE TOMAS DEL TIPO FOTOGRÁFICO

COMUNICACIONES
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

CAPUFE
CAMINOS Y PUENTES FEDERALES

SISTEMA CIRCUITO CERRADO DE OFICINAS CENTRALES Y ÓRGANO INTERNO DE CONTROL ESPECÍFICO
SOLICITUD DE REVISION

FECHA		**FECHA DE REVISION SOLICITADA**	
EXT.			
Nombre del Trabajador (a):			
Puesto o Categoría:		**Número de Empleado (a):**	
Área de Adscripción			

Nombre y firma de la persona Titular de la Subdirección de su Área:

Nombre: | **Cargo:**

JUSTIFICACION DE LA SOLICITUD

SOLICITANTE | **SUBDIRECCIÓN DEL AREA**

FIRMA | **FIRMA**

ANEXO 2

FORMATOS DE SOLICITUD DE SERVICIOS

1. Identificación del Servicio					
Servicio de TI referido	*Internet*	Descripción de la solicitud	*Acceso a VPN*	Justificación de actividades	
Solicitud (alta, baja o cambio) en caso de que aplique	*Alta*	Periodo de vigencia	*10/10/2023 al 10/10/2024*	Fecha	*10 de octubre de 2023*

2. Datos del usuario solicitante					
Número de empleado (a)	*407119*	Nombre completo de la o el solicitante	*Eunice Shirley Moreno Olais*	División	*Oficinas Centrales*
Teléfono / Ext	*3613*	Adscripción	*Subgerencia de Control de Operación de Medios Electrónicos de Pago*	Firma del solicitante	
Sociedad	*CAPUFE*	e-mail	esmoreno@capufe.gob.mx	Puesto	*Superintendente B*
Nivel aprobado		Comentarios adicionales antes de aprobar el servicio		Periodo de vigencia	
Nombre de la o el técnico que recibe la solicitud		Firma de la o el técnico que recibe la solicitud		Número de ticket asignado	

3. Firmas de aprobación					
Nombre de la o el jefe inmediato de la persona solicitante	*María del Pilar Jiménez Carrillo*	e-mail	pjimenez@capufe.gob.mx	Firma de aprobación	
Nombre de la o el responsable del área solicitante	*Lic. Judith Sosa Limón*	e-mail	jsosal@capufe.gob.mx	Firma de aprobación	
Responsable del servicio de Tecnologías de Información	*Gloria Laura Segovia Cruz*	e-mail	gsegovia@capufe.gob.mx	Firma de aprobación	

Nota: ***El periodo de vigencia no debe rebasar el límite de un año***
Antes de imprimir el formato, se tendrán que borrar las instrucciones que la persona usuaria no tenga que llenar (los apartados que están descrito en color rojo)

ANEXO 3

FORMATO DE SOLICITUD PROVEEDOR

1. Identificación del Servicio					
Servicio de TI referido	*Internet*	Descripción de la solicitud	*<Especificar a **detalle** la necesidad de la solicitud>*	Justificación de actividades	*<Justificación de las actividades de acuerdo a las funciones que desempeña en su puesto para la aprobación del servicio>*
Solicitud (alta, baja o cambio)	*Alta*	Periodo de vigencia	*Especificar la duración total que estará activo el servicio <dd/mm/aaaa >*	Fecha	*<Fecha de la solicitud del servicio dd/mm/aaaa>*
Nombre de la o el técnico que recibe la solicitud	*<Nombre de la o el técnico responsable de atender a la persona usuario>*	Firma de la o el técnico que recibe la solicitud	*<Firma de aprobación de la o el técnico que levantará el ticket en la mesa de servicio>*	Número de ticket asignado	*<Número de ticket con el que se va a atender la solicitud>*
2. Datos del usuario solicitante					
Nombre completo de la o el solicitante	*<Capturar el nombre completo de la persona usuaria solicitante>*	Teléfono personal y Ext. de oficina	*<Número personal, extensión telefónica en donde se le pueda localizar>*	Nombre de la Empresa	*<Nombre completo de la empresa>*
Adscripción	*<Nombre del área que solicita petición, Ej. Subdirección de TI>*	Domicilio	*<Domicilio de la empresa>*	e-mail	ejemplo@tuempresa.com.mx
Dirección IP y Puertos	*<Dirección IPy puertos a los que se les proporcionara acceso>*	Características del equipo en la que se usara el internet	*<Marca, modelo y No. de serie del equipo>*	Firma de la persona que usara el servicio de internet	
3. Firmas de aprobación					
Nombre de la o el responsable de la solicitud	*<Nombre completo de la o el responsable de la petición del servicio>*	e-mail	ejemplo@capufe.gob.mx	Firma de aprobación	
Nombre de la o el jefe del responsable del área	*<Nombre de la autoridad máxima de la o el responsable que realiza la petición, Subdirección o Dirección>*	e-mail	ejemplo@capufe.gob.mx	Firma de aprobación	
Responsable del servicio de Tecnologías de Información	*Gloria Laura Segovia Cruz*	e-mail	gsegovia@capufe.gob.mx	Firma de aprobación	

Nota: El periodo de vigencia no debe sobrepasar el límite de un año
Antes de imprimir el formato, se tendrán que borrar las instrucciones que la persona usuaria no tenga que llenar (instrucciones que están descritas en color rojo)

ANEXO 4

SOLICITUD DE VPN

1. Identificación del Servicio					
Servicio de TI referido	*Acceso remoto a la red de CAPUFE (VPN)*	Descripción de la solicitud	*<Especificar a **detalle** la necesidad de la solicitud>*	Justificación de actividades	*<Justificación de las actividades de acuerdo a las funciones que desempeña en su puesto para la aprobación del servicio>*
Solicitud (alta, baja o cambio)	*Alta*	Periodo de vigencia	*Especificar la duración total que estará activo el servicio <dd/mm/aaaa >*	Fecha	*<Fecha de la solicitud del servicio dd/mm/aaaa>*
2. Datos del usuario solicitante					
Número de Empleado (a)	*<Número de empleado (a) identificador único del personal en activo>*	Nombre completo de la o el solicitante	*<Capturar el nombre completo de la persona usuaria solicitante>*	División	*Oficinas Centrales*
Teléfono personal y Ext. de oficina	*<Número personal, extensión telefónica en donde se le pueda localizar>*	Adscripción	*<Área a la que pertenece el usuario solicitante>*	e-mail	ejemplo@capufe.gob.mx
Puesto	*<Puesto de la persona usuaria solicitante>*	Domicilio	*<Domicilio de la o el solicitante en caso de ser equipo CAPUFE o FONADIN>*	Equipo	*<Particular, CAPUFE, FONADIN>*
Sociedad del empleado (a)	*<CAPUFE,FONADIN,EXTERNO>*	Características del equipo	*<Marca, modelo y No. de serie del equipo>*	Firma de la o el usuario solicitante	
Nombre de la o el técnico que recibe la solicitud	*<Nombre de la o el técnico responsable de atender a la persona usuaria>*	Firma de la o el técnico que recibe la solicitud	*<Firma de aprobación de la o el técnico que levantará el ticket en la mesa de servicio>*	Número de ticket asignado	*<Número de ticket con el que se va a atender la solicitud>*
3. Firmas de aprobación					
Nombre de la o el jefe inmediato del solicitante	*<Nombre completo de la o el jefe inmediato del solicitante del servicio>*	e-mail	ejemplo@capufe.gob.mx	Firma de aprobación	
Nombre de la o el responsable del área	*<Nombre de la autoridad máxima responsable del área al que pertenece la persona usuaria, Subdirección o Dirección>*	e-mail	ejemplo@capufe.gob.mx	Firma de aprobación	
Responsable del servicio de Tecnologías de Información	*Gloria Laura Segovia Cruz*	e-mail	gsegovia@capufe.gob.mx	Firma de aprobación	

Nota: El periodo de vigencia no debe sobrepasar el límite de un año

Antes de imprimir el formato, se tendrán que borrar las instrucciones que la persona usuaria no tenga que llenar (instrucciones descritas en color rojo)

ANEXO 5

SOLICITUD DE ALTA, BAJA O CAMBIO DE USUARIOS (AS) PARA APLICATIVO DE CÓMPUTO

Datos Generales			
Aplicativo de Cómputo:	*[Indique el nombre del aplicativo de cómputo objeto de la presente solicitud]*	Fecha de Solicitud:	*[dd/mm/aaaa]*

Datos de Usuarios (as) y Permisos										
No.	No. Empleado (a)	Nombre Completo	Correo Electrónico	Número Ext.	Área Adscrita	Centro de Trabajo	Solicitud	Usuario (a)	Módulos	Permisos
1	*[No. de empleado]*	*[Nombre completo del personal que requiere un alta, baja o cambio de usuario]*	*[correo electrónico: ej. jperez@, no se requiere el dominio]*	*[No. Ext.]*	*[Área a la que está adscrita la persona]*	*[Lugar de trabajo, ej. Oficinas Centrales]*	*[Alta, baja o cambio]*	*[En el caso de que ya exista el usuario, especificarlo aquí]*	*[Describa los módulos o accesos a los que requiere dentro del aplicativo de cómputo]*	*[Consulta, Administración, Gestión, Edición o cualquier tipo de permiso que tendrá la o el usuario]*
2										
3										

Gobierno			
Responsabilidad	Nombre	Cargo	Firma
Solicitante	*[Nombre completo de quien realiza la solicitud.]*	*[Cargo de quien realiza la solicitud, debe ser un nivel **subgerencia** o **gerencia**.]*	
Autoriza	*[Nombre completo de quien autoriza la solicitud del Área requirente.]*	*[Cargo de quien realiza la autorización, debe ser un nivel superior del solicitante, es decir **gerencia** o **subdirección**.]*	
Validación de los datos de la solicitud (STI).	*[Nombre completo de quien valida la solicitud y aplica la misma por parte de la STI.]*	*[Cargo de quien valida y aplica la solicitud, debe ser un nivel **subgerencia** o **gerencia**.]*	
VoBo (STI).	*[Nombre completo de quien da el visto bueno a la solicitud por parte de la STI.]*	*[Cargo de quien da el visto bueno de la solicitud, debe ser un nivel **gerencia** o **subdirección**.]*	