DICONSA

MANUAL DE PROCEDIMIENTOS DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Clave: VSS-UAF-PR-001 **No. de Revisión: 00**

Emisión Original: 10-11-2022 **Fecha: 10-Noviembre-2022**

ÍNDICE GENERAL

I. INTRODUCCIÓN

Diconsa, S.A. de C.V., es una empresa de participación estatal mayoritaria sectorizada a la Secretaría de Desarrollo Rural (SADER) que pertenece al Sector 08 Agricultura, Ganadería y Desarrollo Rural. Tiene el propósito de contribuir a la superación de la pobreza alimentaria, mediante el abasto de productos básicos y complementarios a localidades rurales de alta y muy alta marginación, con base en la organización y la participación comunitaria.

Diconsa atiende cerca de 26 mil tiendas en todo el país y para cumplir con su objetivo cuenta con más de 300 almacenes rurales y centrales, 3 mil 691 mil unidades asignadas a sucursales que cada día recorren miles de kilómetros de carreteras y terracerías, de tal forma que completarían un viaje de ida y vuelta a la luna.

Una de sus principales funciones es hacer negociaciones para la adquisición de los principales productos básicos que los mexicanos consumen en zonas rurales tales como maíz, frijol, arroz, azúcar, leche, café, harina de maíz, harina de trigo, sal de mesa, aceite, chocolate, chile, atún, sardina, galletas, pasta para sopa, abarrotes y mercancías en general.

Con la finalidad de cumplir con su objetivo, Diconsa, S.A. de C.V. hace uso de las Tecnologías de la Información, siendo éste un activo suministrado a los integrantes de la entidad para contribuir al cumplimiento de sus actividades y acciones encomendadas a sus funciones. Toda información transmitida por medio de las tecnologías de la información será tratada como información relacionada con la Entidad y deberá estar alineada a las políticas, descritas más adelante.

Con el transcurso del tiempo las cuentas de usuarios(as), equipos y servicio requieren ser modificadas derivadas de un evento de alta, baja o cambio de adscripción. Los mecanismos y herramientas del directorio activo ayudan a identificar las cuentas de equipos y usuarios(as) que se han deshabilitado o expirado. Por lo tanto, basados en las políticas de mantenimiento del directorio activo, se pueden depurar las cuentas de manera efectiva y eficiente.

El presente documento fortalece la cultura informática de los usuarios de la Entidad y es un apoyo para incrementar la eficiencia de los mismos, además, se aborda el concepto de "Seguridad para Internet", enunciando los programas y soluciones que protegen la Red Nacional de Diconsa, S.A. de C.V. y su interacción con Internet, e integra el procedimiento para el ejercicio de las funciones asignadas a la Gerencia de Sistemas, respecto a las altas, bajas y cambios de cuentas de usuarios(as), establecer políticas de uso y configurar perfiles lo cual permite mantener en óptimas condiciones la infraestructura tecnológica de Diconsa, S.A. de C.V., así como apoyar a enlaces informáticos ubicados en las diferentes entidades para la atención de usuarios(as) locales en cumplimiento eficiente de las acciones operativas que demandan las funciones encomendadas mediante el uso de tecnologías de la información.

II. OBJETIVOS

- Este manual tiene como objetivo proporcionar a los usuarios de Diconsa, S.A. de C.V. una guía de buenas prácticas para el uso responsable de los Servicios de Tecnologías de la Información.

- Establecer la normatividad interna que regule los procedimientos para la prestación oportuna y eficiente de los servicios de TIC y seguridad de la información que coadyuven en el cumplimiento de los objetivos y metas institucionales de la Entidad.

- Garantizar con honestidad y transparencia el uso de los activos y servicios de tecnologías de la información.

- Coadyuvar con el cumplimiento de los objetivos y metas institucionales.

III. GLOSARIO

Administrador	Refiere a la Gerencia de Sistemas.
Administrador del Servicio	Refiere al área que solicitó el sistema.
Acceso	Es el resultado positivo de una autentificación, en el Directorio Activo o Aplicación, este permitirá que el/la usuario(a) conforme a su perfil y privilegios pueda suministrar, actualizar o consultar información.
Acceso remoto	Es poder acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa.
Área administradora	Área administrativa encargada de alimentar con su propia información el sistema requerido y/o asignado.
Almacenar	Guardar datos en dispositivos externos sean de hardware, software o en la nube, dedicados a este fin.
Alta	Registrar una nueva cuenta de el/la usuario(a) en el directorio activo para acceso a los servicios y sistemas institucionales de Diconsa, S.A. de C.V., según sea el caso.
Área responsable (AR)	Refiere a la Gerencia de Sistemas
Ataque	Método por el cual un individuo o grupo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (equipo de cómputo, aplicación, red privada, etcétera).
Autenticar	Es el acto de establecimiento o confirmación de algo (o alguien) como auténtico, la autenticación de una persona a menudo consiste en verificar su identidad.
Baja	Eliminar una cuenta de la persona usuaria en el directorio activo.
Blog	En español bitácora digital. Sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente.
Cambio	Realizar ajustes en la información y registro de una cuenta de el/la usuario(a) en el directorio activo.
Chat	Término proveniente del inglés que en español equivale a "charla", también conocido como cibercharla. Se refiere a una comunicación escrita realizada de manera instantánea mediante el uso de un software y a través de Internet entre dos o más personas, ya sea de manera pública a través de los llamados chats públicos (mediante los cuales cualquier persona usuaria puede tener acceso a la conversación) o privados, en los que se comunican dos o más personas autorizadas.
Confidencialidad de la Información	Conjunto de reglas que limita el acceso y la divulgación de la información a personas o sistemas que no se encuentran autorizados.
Contraseña	Código secreto que se introduce en un equipo de cómputo para poder accionar o para acceder a ciertas funciones informáticas.

Cuenta de usuario	Información que se compone por un nombre de la persona usuaria y una contraseña registrados en el directorio activo, y que permite acceder a los servicios y sistemas institucionales de Diconsa, S.A. de C.V.
Denegar	No conceder una solicitud. No otorgar una demanda, dar una respuesta negativa a un pedido.
Descargar	Proceso mediante el cual se transfiere información (datos, programas. etc.) de un equipo de cómputo a otro por medio de ciertos protocolos (ejemplo FTP), especialmente a través de Internet u otra red informática para ejecutarlos o almacenarlos.
Diconsa	Diconsa S.A. de C.V.
Directorio Activo (DA)	Es el servicio de directorio de una red de Windows; este se convierte en un medio de organizar, controlar y administrar centralizadamente el acceso a los recursos de la red, además, separa la estructura lógica de la organización (dominios) de la estructura física (topología de red).
Discriminación	Trato de inferioridad hacia una persona o congregación por causa de raza, origen, ideas políticas, religión, posición social o situación económica.
Disponibilidad de la Información	Es una garantía de acceso confiable a la información por parte de personas autorizadas.
Dominio	Red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.
eMule	Programa Peer-to-Peer que permite descargar y compartir archivos con el resto de las personas usuarias conectadas a la red.
Enlace de datos	Vínculo físico entre una oficina y otra. En el caso de Sucursales, Unidades Operativas y Almacenes de Diconsa, S.A. de C.V., todos se conectan con Oficinas Centrales y desde ese punto salen hacia Internet.
Enlace Informático	Personal capacitado para la atención de inconvenientes en los servicios de TIC´s.
Entregable	Productos intermedios que se generan en las fases o procesos y permiten evaluar o evidenciar la marcha del proyecto mediante comprobaciones de requerimientos o comprobaciones de entrega.
Guía	Documento que da la orientación, instrucciones, procedimientos y consejos sobre determinado tema o materia.
Hacking	Acción de irrumpir o entrar de manera forzada a un equipo de cómputo, sistema o red, explorando o buscando las limitantes de un sistema o código de un equipo informático.
Hitos	Punto de control en alguna fase de la ejecución de un proyecto, el cual permite validar que el avance sea de acuerdo a lo planificado.
ICQ	Cliente de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes instantáneos a otras personas usuarias conectadas a la propia red de ICQ. También permite el envío de archivos, videoconferencias y charlas de voz.
Input	Conjunto de datos que se introducen en un sistema o un programa informático.
Integridad de la Información	Es la garantía de que la información es confiable y precisa, y que ésta se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

Internet	Es un conjunto descentralizado de redes de comunicación y computadoras interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Es un conjunto de redes en todo el mundo que conectadas entre sí pueden transmitir información digital entre sus dispositivos con ayuda de protocolos de comunicación.
Intranet	Red de servidores privados que utiliza tecnología de Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales, formada por un número determinado de servidores de acceso restringido sólo a personas autorizadas.
Intransferible	Que no puede ser dado o transferido a otra persona.
Kazza	Aplicación de intercambio de archivos Peer-to-Peer que emplea el protocolo Fast Track, especialmente usado para el intercambio de archivos de música MP3 en internet.
Kick off	Punto de partida de un proyecto que compromete a varias personas o diferentes departamentos, y que se acomete convocando a todas ellas para que participen en una reunión simultánea con un formato muy cuidado.
Lesivos	Acciones con fines maliciosos que puedan perjudicar a terceros, así como causar lesión, daño en el orden moral y jurídico.
Lineamientos	Conjunto de acciones específicas que determinan la forma, lugar y modo para llevar a cabo una política.
Log	Registro en un archivo secuencial de todos los eventos o acciones que afectan a un sistema o base de datos, de esta forma se constituye una evidencia del comportamiento paso a paso de las actividades en un momento exacto (fecha, hora, minuto, segundo).
Messenger	Aplicación que permite el intercambio en tiempo real de mensajes entre una o más personas usuarias en forma de texto.
Metodología	Conjunto de conocimientos encargados de elaborar, definir y sistematizar un conjunto de técnicas, métodos y procedimientos que se deben seguir durante el desarrollo de un proyecto para la producción de los productos o servicios.
Monitorear	Gestión y supervisión para controlar la actividad de las personas usuarias, programas, páginas Web y accesos a la red, la cual proporciona información sistemática, uniforme y fiable por medio de dispositivos tecnológicos.
Morpheus	Es una completa herramienta de intercambio de archivos Peer to- Peer que permite compartir todo tipo de ficheros multimedia.
MP3	Formato de compresión de audio digital patentado que usa un algoritmo con pérdida para conseguir un menor tamaño de archivo. Es un formato de audio usado para música tanto en equipos de cómputo como en reproductores de audio portátil.
MSD	Mesa de servicio de Diconsa, S.A. de C.V.
Navegador	Software que las personas usuarias utilizan para poder visitar sitios Web a través de Internet.
Nudismo	Práctica por parte de personas que se presentan desnudos, generalmente en público.

Online	Cualquier servicio que se puede ver o utilizar a través de un navegador, por ejemplo: servicio de trámites, e-Gobierno, Intranet, bibliotecarios, etc.
Pederastia	Práctica delictiva del abuso sexual de una persona hacia los menores de edad.
Phishing	El phishing es un delito que utiliza la ciberdelincuencia por medio de correos electrónicos suplantando la identidad de organizaciones o instituciones públicas.
Pornografía	Material que muestra cuerpos humanos desnudos, escenas explicitas de sexo o aquello que involucre o incite a relaciones de tipo sexual en cualquiera de sus clasificaciones.
Programa	Conjunto de instrucciones que, una vez ejecutadas, realizarán una o varias tareas en una computadora; también conocido como software o aplicación.
Proselitismo	Empeño o afán con que una persona o una institución tratan de convencer y ganar seguidores o partidarios para una causa o una doctrina.
Protocolo	Conjunto de reglas usadas por las computadoras para comunicarse unas con otras a través de una red. Puede ser definido como el estándar que define la sintaxis, semántica y sincronización de la comunicación entre estas. Los protocolos pueden ser implementados por hardware, software o una combinación de ambos.
Proxy	Punto intermedio entre un equipo informático conectado a Internet - y el servidor que está accediendo. Cuando navegamos a través de un proxy en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor al que queremos acceder y nos devuelve el resultado de la solicitud.
Proyecto	Servicio temporal que se lleva a cabo para crear un producto, servicio o resultado único, el cual tiene un inicio y un fin, mismo que se contempla alcanzar dentro de un tiempo determinado.
Puertos	Forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir entre dispositivos periféricos.
Punto a punto (P2P)	Del inglés Peer-to-Peer. Red descentralizada que no tiene clientes ni servidores fijos, sino que tiene una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red. Cada nodo puede iniciar, detener o completar una transacción compatible. Contrasta con el modelo cliente-servidor.
Racismo	Forma de discriminación de las personas por tono de piel u otras características físicas de las personas, de tal modo que unas se consideran superiores a otras.
Real Player	Aplicación para reproducir música y videos en varios formatos multimedia, incluyendo MP3, MPEG-4, QuickTime, etc.
Recertificación	Procedimiento que permite certificar periódicamente que los usuarios todavía utilizan las cuentas y perfiles asignados.
Red	Conjunto de dispositivos computacionales, electrónicos y de comunicación interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación y, en su conjunto más amplio, forman el enmarañado mundial.
Red local	Un sistema de transmisión de datos que permite compartir recursos e información por medio de equipos de cómputo o redes de éstos que comparten el mismo dominio o pertenecen a una misma organización, así se crea un sistema de comunicaciones capaz de facilitar el intercambio de datos informáticos, voz, difusión de video y cualquier otra forma de comunicación electrónica.

Redes Sociales	Comunidades virtuales en sitios web que ofrecen servicios y funcionalidades de comunicación diversas para mantener en contacto a las personas usuarias de la red. Se basan en un software especial que integra numerosas funciones individuales: blogs, foros, chat, mensajería, etc. en una misma interfaz y que proporciona la conectividad entre diversos usuarios(as) de la red.
Road Map	Mecanismo flexible de integración y sincronización de tendencias externas y planes internos, mediante el cual las organizaciones pueden alinear y ajustar la forma de poner en práctica su estrategia de manera sistemática y gradual.
Seguridad de la Información	Conjunto de medidas preventivas o correctivas que permiten a la Entidad resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
Seguridad para Internet	Medidas de protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida) al momento de conectarse a la red pública llamada Internet. Son también servicios y estrategias para resguardar el intercambio de información y proporcionar seguridad en toda la red protegiendo los servidores con acceso a Internet y a redes privadas.
Sistema	Es el conjunto de partes interrelacionadas, hardware, software, dispositivos electrónicos inteligentes, procesadores, memoria, sistemas de almacenamiento e inclusive, el recurso humano que permite procesar información y hacer posible la comunicación entre dispositivos en una red y fuera de ella.
Sistema de Filtrado de Contenido	Programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web. El filtro de contenido determina qué contenido estará disponible en una máquina o red particular. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable.
Sistema de Información	Sistema que procesa información mediante el uso de interfaces para la captura de datos.
Sitio WEB falso	Copias falsas de los sitios WEB conocidos por las victimas con la finalidad de robar nombres de usuarios y contraseñas, así como también en muchas ocasiones información financiera
SMISHING	SMS (mensajes de texto por celular) en los que se solicita dar clic en enlaces, llamar a un número en específico o responder con códigos confidenciales.
Software	Conjunto de componentes lógicos que permiten que los programas funcionen adecuadamente facilitando la interacción de los componentes físicos y el resto de las aplicaciones para realizar tareas específicas proporcionando una interfaz con la persona usuaria.
SPAM	Correos electrónicos no deseados con remitentes desconocidos y que en ocasiones contienen archivos adjuntos o enlaces que vulneran la seguridad de nuestros equipos y que permiten propagar programas malware ("software malicioso") y robar información.
Sponsor	Coordinado, patrocinador de un proyecto, o conjunto de personas de nivel superior responsable del éxito de un proyecto quienes ofrecen la orientación y recursos necesarios al equipo en medida de lo posible.
Sprint	Tiempo fijo repetible durante el cual se crea un producto "Terminado" del valor más alto posible.

Stakeholders	Personas u organizaciones que tienen relación con las actividades a ejecutar en un proyecto.
Telefonía por Internet	Grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada).
Tráfico excesivo de red	Cantidad excesiva de megabytes o paquetes de datos transferido que se produce en una red, servidor web o en un sitio web en un determinado período de tiempo, ya sea por descargas, cargas de información o peticiones, que pueden provocar colisiones en la misma, algún contratiempo o daño lógico.
Transmitir	Enviar archivos o información en cualquier formato de tipo digital desde un emisor a un receptor a través de un medio de transmisión como lo es una red local o extendida (Internet).
Túnel	Efecto de utilizar ciertos protocolos de red que encapsulan a otro protocolo. Así, el protocolo A es encapsulado dentro del protocolo B de forma que el primero considera al segundo como si estuviera en el nivel de enlace de datos. La técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría.
Usuario(a)	Persona que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático.
Ventana	Área visual que contiene algún tipo de interfaz de la persona usuaria, mostrando la salida y permitiendo la entrada de datos para uno de varios procesos que se ejecutan simultáneamente.
Ventanas emergentes	Ofertas o premios falsos que solicitan datos importantes de el/la usuario(a) y robar información
Virus	Programas de tipo Malware de equipo de cómputo que se reproducen a sí mismos e interfieren con el hardware de una computadora o con su sistema operativo. Tienen por objeto alterar el funcionamiento normal de la computadora, sin el permiso o el conocimiento de la persona usuaria.
VISHING	Llamadas provenientes de Falsos centros de atención telefónica para obtener información confidencial

IV. MARCO LEGAL

A. Constitución Política de los Estados Unidos Mexicanos.

B. Leyes

- Ley Orgánica de la Administración Pública Federal. Vigente.
- Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público. Vigente.
- Ley General de Archivos. Vigente.
- Ley Federal de Entidades Paraestatales.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Responsabilidades Administrativas.

C. Estatuto

- Estatutos Sociales de Diconsa, S.A. de C.V.

D. Acuerdos

- 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.

E. Otras disposiciones

- Manual de Organización de DICONSA S.A. de C.V.
- Manual de Organización de SEGALMEX
- Políticas de los Servicios de TI DICONSA S.A. de C.V.

V. ALCANCE

A. Todas las Áreas de Oficinas Centrales.

B. Sucursales, Unidades Operativas, Oficinas Regionales, Almacenes Centrales y Rurales.

VI. NORMAS GENERALES

1. Es responsabilidad de las personas servidoras públicas de Diconsa, S.A. de C.V., en el ámbito de su competencia, cumplir las disposiciones contenidas en el presente Manual.

   Lo anterior, toda vez que cualquier proceso sancionatorio corresponde a la autoridad competente.

2. La Gerencia de Sistemas será responsable de la aplicación y seguimiento de las normas contenidas en el presente documento.

3. Los titulares de las diversas áreas deberán notificar a la brevedad cualquier alta, baja o cambio de servicios de TIC's del personal a su cargo.

4. La Gerencia de Recursos Humanos deberá de notificar a la Gerencia de Sistemas la baja del personal de base, confianza y honorarios, al menos una vez al mes.

5. Los servicios de TIC's se encargarán de brindar la infraestructura de comunicaciones, hardware, software y seguridad que permitirán un óptimo desempeño del flujo de la información en la institución de forma interna y externa.

6. La administración de los servicios de TIC's, se realizará de manera conjunta entre los prestadores de servicio y la Gerencia de Sistemas.

7. La Gerencia de Sistemas será la encargada de administrar los servicios de TIC's dentro de la dependencia.

8. La Gerencia de Sistemas será responsable de monitorear revisar y analizar en cualquier momento toda la actividad de accesos y consultas que las personas usuarias realizan a las diferentes fuentes y páginas de Internet, utilizando las herramientas de seguridad de este servicio.

9. La Gerencia de Sistemas se encargará de ejecutar, previa solicitud de las áreas requirentes la autorización de los servicios de TIC's en la entidad de acuerdo a la disponibilidad y factibilidad del requerimiento.

10. Por razones de buen servicio, la Gerencia de Sistemas tendrá la facultad de "limitar" cualquier tipo de contenido NO útil para Diconsa, S.A. de C.V., contenidos como video online, radio online, TV online, descarga de películas o algún otro programa podrían quedar restringidos para asegurar la entrega de las aplicaciones institucionales, privilegiando lo que es esencial para el desarrollo de las funciones del personal, y bloqueando o rechazando todo aquello que representa un riesgo y que no está acorde con el desarrollo de las labores del personal.

11. El directorio activo será la herramienta que permitirá la organización y gestión de los recursos de red, de servidores y todo lo que ello implica: personas usuarias, servicios, puestos, impresoras, permisos y equipos de escritorio de la entidad. Es por tanto el directorio activo el que almacenará toda la información de los objetos que componen la red de Diconsa, S.A. de C.V. Esto permitirá centralizar en un único punto la gestión de red de administración de personas usuarias y contraseñas.

12. El servicio de directorio activo también ofrecerá la ventaja de tener un único punto de entrada para las personas usuarias de la red de Diconsa, S.A. de C.V. Las personas usuarias podrán buscar y usar recursos sin conocer el nombre o la ubicación exacta de estos. Igualmente, se podrá administrar toda la red con una vista lógica y unificada de la entidad y de sus recursos.

13. Otras ventajas del directorio activo se resumen a continuación:

    Organización: Permitirá crear grupos para facilitar la administración. Ejemplo, se puede crear un grupo con las personas usuarias de un área específica.

    Permisos: Permitirá el control desde un sólo punto, de los permisos a los recursos de la red. Ejemplo: se puede asignar a una carpeta permisos de lectura a un área, mientras que

otra área no puede entrar y ciertas personas tienen control total.

Autentificación: Cualquier persona usuaria podrá entrar en otro equipo de la red con su usuario y clave, y tendrá los permisos que se le hayan asignado, es decir, los permisos se asignan por clave de usuario no por equipo.

Políticas: Se podrá controlar el comportamiento de los equipos y permisos de los/las usuarios(as) de forma muy concreta. Ejemplo: cambiar el fondo de pantalla del escritorio en todos los equipos, o la caducidad de las contraseñas de los/las usuarios(as).

Escalabilidad: Es un sistema que funcionará en un sólo servidor y para miles de personas usuarias repartidos por varias sedes y varios servidores balanceando la carga.

Autentificación externa: Permitirá que otras aplicaciones lean los datos, Ejemplo: una aplicación de presupuesto no requiere otra clave para entrar, lee la de la persona usuaria en el directorio activo.

Replicación: Implementará características para la replicación de todos los datos entre servidores del directorio activo. Ejemplo: si la empresa tiene dos sedes, las personas usuarias con sus permisos se sincronizan solos automáticamente.

14. Las cuentas institucionales de las personas usuarias de Diconsa, S.A. de C.V., representan e identifican a cada persona que utiliza servicios de red, aplicaciones y sistemas dentro de la Entidad.
15. El registro y administración de cuentas de usuario, se realizará a través del directorio activo y cada módulo de administración de personas usuarias de los sistemas de información institucionales, así como de las políticas que más adelante se especifican.
16. El módulo de administración de personas usuarias permitirá las siguientes acciones:
    - Autenticar la identidad de la persona usuaria. Una cuenta permite que la persona usuaria inicie sesión en algún servicio o sistema de información institucional que corresponda a su actividad. La persona usuaria que inicia sesión debe hacerlo proporcionando su cuenta de usuario y contraseña únicos, los cuales corresponden a su cuenta de correo institucional.
    - Autorizar o denegar el acceso a las opciones del servicio o sistema de información institucional: Después de la persona usuaria se autentica, se le concede o se le deniega el acceso a las opciones de los diferentes módulos del servicio o sistema de información institucional en función de los permisos definidos que la cuenta tenga asignados, con base al perfil autorizado por el área administradora del Sistema Institucional.
17. Las áreas administradoras de los sistemas serán las responsables de autorizar el acceso de usuarios a los sistemas.
18. Las áreas administradoras de los sistemas deberán documentar los roles y permisos otorgados a las personas usuarias con base al puesto, funciones y responsabilidades que desempeñen, asimismo, el nombre y puesto de los usuarios deberán coincidir con la plantilla del personal de Diconsa, S.A. de C.V. generada por el área de Recursos Humanos.
19. Las áreas administradoras de los sistemas deberán realizar revisiones periódicas a efecto de evitar lo siguiente:
    - Segregación de funciones en los sistemas.
    - Cuentas activas en los sistemas, cuando el personal usuario de la cuenta ha causado baja en Diconsa, S.A. de C.V.

- Cuentas que no tengan asignado un responsable.

20. Las áreas administradoras de los sistemas deberán realizar y documentar la recertificación de los perfiles de acceso de las personas usuarias.

21. Cada persona usuaria será la única responsable del uso de la cuenta de directorio activo asignada, así como del uso de sus contraseñas o claves de acceso, por lo que su mal uso podrá ser sancionado en términos de la normatividad aplicable.

22. Estará prohibido el acceso a sitios y páginas relacionados con contenido sexual, violento, discriminatorio, música, radio, televisión, fraudes, juegos, actividades ilegales de cualquier tipo, chats, redes sociales de cualquier tipo, contenidos maliciosos, virus, entretenimiento, tarjetas de felicitación, drogas, telefonía por Internet, acceso remoto, apuestas, hacking o sitios reconocidos como inseguros, entre otros, los cuales pueden poner en riesgo la integridad y confidencialidad de la información de la Entidad. La mayor parte de estas páginas se encuentran bloqueadas, a través del Sistema de Filtrado de Contenidos de Internet que forma parte del protocolo de seguridad de internet.

VII. POLÍTICAS GENERALES

1. La Gerencia de Sistemas será responsable de la revisión, aplicación y seguimiento de las políticas contenidas en el presente documento, haciendo una revisión y/o actualización por lo menos una vez al año con la finalidad de mantenerlas vigentes o cuando se presente cualquiera de los siguientes casos:
   - Por asignación de nuevas funciones y responsabilidades.
   - Por el establecimiento de nuevos métodos o sistemas de trabajo.
   - Como resultado del proceso de simplificación administrativa.
   - Como resultado de cambios en la normatividad aplicable.
2. La persona usuaria de Internet es la única responsable de la utilización que se haga del servicio que tiene asignado, así como de la información y/o programas que se "carguen" y "descarguen" desde Internet, en el equipo de cómputo que utilice.
3. Las personas usuarias deben acceder a Internet usando el navegador que se provee en sus respectivas computadoras. El navegador por defecto es el Microsoft Internet y en la imagen institucional se incluye Google Chrome como una alternativa autorizada.
4. El servicio se asigna de forma personalizada a las personas usuarias; es intransferible. La Gerencia de Sistemas se reservará el derecho a cancelar el acceso al servicio, si la persona usuaria incurre en las siguientes faltas:
   a. Que la persona autorizada se encuentre ausente y otra persona utilice su equipo para acceder al servicio.
   b. Publique cualquier tipo de información perteneciente a Diconsa, S.A. de C.V. en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.
   c. Publique comentarios no profesionales en foros públicos, sitios de chat, Weblogs (Blogs), correo electrónico, o cualquier otro medio de publicación en Internet.
   d. Participe en cualquier actividad ilegal o criminal.
   e. Realice solicitudes no autorizadas de dinero o la operación de negocios personales.
   f. Obtenga acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad.
5. La Gerencia de Sistemas podrá cancelar en cualquier tiempo los accesos de las personas usuarias de forma temporal y/o definitiva incluso sin previo aviso, cuando la utilización del servicio represente un riesgo para la operación y/o seguridad de la información de la Entidad, por ejemplo: Infecciones por virus descargados desde Internet o bien, la generación de tráfico excesivo de red hacia Internet por un usuario, etc.
6. De forma excepcional, se podrá otorgar el acceso a los sitios relacionados con: redes sociales, radio, televisión, etc. siempre que éstos estén directamente relacionados con las funciones del área. Para ello, el Titular del área deberá solicitarlo mediante oficio a la Gerencia de Sistemas y anexar la justificación para dicho acceso.
7. Queda estrictamente prohibido descargar de Internet e instalar en las computadoras de Diconsa, S.A. de C.V., software de red llamado "punto a punto" (Peer to Peer) para descargar música, juegos, videos, entretenimiento online como Facebook, Twitter, Instragram, Tik-tok y/o cualquier red social; Streaming ya que estos habilitan puertos o crean "túneles" permanentes entre la red local e Internet, lo que se traduce en un riesgo para la seguridad. Ejemplos: Kazza,

Imesh, Morpheus, Limewire, eMule, Real Player, ICQ, Messenger, entre otros. El Sistema de Filtrado de Contenidos de Internet, bloqueará los programas con los cuales se puedan descargar páginas para instalar el software de red llamado "punto a punto" (Peer to Peer).

8. Se prohíbe descargar programas diversos de Internet ajenos a las actividades de trabajo, y aquellos cuyo contenido esté relacionado con los numerales 6 y 8 que anteceden, incluyendo aquellos que no sean parte del software autorizado y de uso institucional, ya que representan un riesgo para la seguridad.

   Si derivado de las funciones del área, se requiere la utilización de un programa o software específico, el titular de ésta deberá solicitar mediante oficio la autorización de la Gerencia de Sistemas para la determinación de su procedencia según el caso particular.

9. Queda estrictamente prohibido el uso de programas denominados "Proxy's", y/o cualquier otro similar cuyo fin sea evadir los sistemas de seguridad de Internet de la entidad.

   El uso de esta clase de programas es motivo para cancelar de manera definitiva el servicio al usuario que incurra en estas acciones, así como la notificación de esto al Titular del área del mismo.

10. El uso y/o acceso indiscriminado y sin justificación del servicio de Internet por parte de los usuarios durante el horario de labores, puede ser motivo de cancelación temporal o definitiva del servicio.

11. Se tomarán las medidas necesarias de prevención y seguridad que, una vez concluida la consulta de información en Internet, se cierren totalmente las ventanas y sesiones en sitios bancarios, financieros u otra donde se maneje información confidencial.

12. Quedará prohibido a todas las personas usuarias utilizar el servicio con fines o efectos ilícitos, lesivos de los derechos e intereses de terceros, o de cualquier forma en la que podrán dañar, inutilizar, sobrecargar o deteriorar los recursos de Diconsa, S.A. de C.V.

    Este tipo de acciones será motivo para cancelar definitivamente el servicio, notificando al titular del área de la persona usuaria y dando aviso al Órgano Interno de Control de la entidad para que tome las medidas conducentes.

13. En los casos de bloqueo o suspensión del acceso a las personas usuarias, la Gerencia de Sistemas notificará al titular del área correspondiente las razones que motivaron dicha acción, de conformidad con el "Procedimiento de Monitoreo de Uso de Internet.

14. Estará estrictamente prohibido para todas las personas usuarias, descargar material (incluyendo software) que cause cualquier acción de violación de la propiedad intelectual de terceros, derechos de privacidad, publicidad o cualquier otro similar que se haga a través del servicio de Internet de Diconsa, S.A. de C.V.

    Este tipo de acciones será motivo para cancelar definitivamente el servicio, notificando al titular del área del usuario y dando aviso al Órgano Interno de Control de la Entidad para que tome las medidas conducentes.

15. Quedará totalmente prohibido a las personas usuarias, el uso del internet para almacenar, publicar, desplegar, transmitir, anunciar datos e información relacionada con actos de proselitismo político y partidista, discriminación, racismo, material potencialmente ofensivo, incluyendo bromas de cualquier tipo, prejuicios, menosprecio o acoso explícito, uso personal y cualquier otro que no esté relacionado con las funciones laborales.

    Este tipo de acciones será motivo para cancelar definitivamente el servicio, notificando al titular del área de la persona usuaria y dando aviso al Órgano Interno de Control de la Entidad para que tome las medidas conducentes.

16. Como parte de las herramientas tecnológicas de apoyo a sus funciones, el personal que labora

en Diconsa, S.A. de C.V. tiene la posibilidad de contar con un equipo de cómputo y aquellos accesorios (cámara, micrófono, bocinas, etc.) que se autoricen para el desarrollo de sus funciones, normalmente con conexión a la red de datos de Diconsa, S.A. de C.V. y una cuenta de usuario de directorio activo. Adicionalmente, la persona usuaria puede contar con una dirección de correo y un buzón electrónico donde almacenar sus mensajes.

17. La persona usuaria será responsable del resguardo y cuidado del equipo de cómputo y de los accesorios asignados.

18. En caso de robo o extravío del equipo de cómputo y/o los accesorios asignados, la persona usuaria será el responsable de levantar el acta correspondiente ante el Ministerio Público y deberá hacer de conocimiento por escrito adjuntando copia de la respectiva acta a la Gerencia de Sistemas para los efectos administrativos y legales que procedan.

19. La persona usuaria de la cuenta de correo electrónico deberá de almacenar sus mensajes en el equipo de cómputo utilizando un repositorio local para tales efectos y depurando el buzón de correo electrónico de mensajes que tengan más de un mes de antigüedad con el fin de no saturar el espacio asignado para cada buzón.

20. La cuenta de usuario es personal e intransferible, por lo tanto, la persona que la utiliza es la única responsable del uso que se haga de la misma, así como de la información que genere y/o intercambie a través de ella.

    El uso indebido de la cuenta ocasionara una suspensión inmediata de la cuenta.

21. El uso de la cuenta de acceso es de carácter institucional y de apoyo a las funciones que la persona usuaria desempeña en Diconsa, S.A. de C.V., por lo que no debe utilizarse con otros fines ajenos a dichas funciones.

22. Quedará prohibido a todas las personas usuarias utilizar el acceso con fines o efectos ilícitos, lesivos de los derechos e intereses de terceros, o de cualquier otra forma que pueda dañar, inutilizar o deteriorar los recursos informáticos de Diconsa, S.A. de C.V.

23. Estará estrictamente prohibida cualquier acción de violación de la propiedad intelectual de terceros, derechos de privacidad, publicidad o cualquier otro similar que se haga a través de la cuenta de usuario institucional de la entidad.

24. Quedará totalmente prohibido el uso de este acceso para publicar, desplegar, transmitir y/o anunciar datos e información relacionado con actos de proselitismo político y partidista.

25. Estará prohibido, el uso de la cuenta de acceso para almacenar, publicar, desplegar, transmitir, anunciar datos e información relacionada con pornografía, discriminación, racismo y cualquier otro fin a los relacionados con las funciones de la institución.

26. Se prohíbe alterar a través de la cuenta de usuario, la configuración de las herramientas y servicios que se utilizan en el equipo de cómputo asignado al personal para sus funciones.

    La única excepción será cuando la Gerencia de Sistemas solicite a la persona usuaria que aplique ajustes, actualizaciones y otros en las configuraciones de los servicios y/o programas del equipo de cómputo asignado.

27. En caso de que la persona usuaria tenga requerimientos relacionados con su cuenta, como: cambios de contraseña, permisos y/o accesos especiales, alta de otros servicios asociados como correo electrónico, mensajería instantánea, etc., deberá solicitarlos a la Gerencia de Sistemas a través de la mesa de servicio de Diconsa, S.A. de C.V., donde se registrará un ticket para ser atendido.

28. La Gerencia de Sistemas será la responsable en monitorear, revisar y analizar en cualquier momento toda actividad relacionada con la utilización de las cuentas de usuario, con el fin de solucionar problemas con el servicio, así como detectar y/o solucionar amenazas o elementos

de peligro para la seguridad e integridad de la información.

29. La Gerencia de Sistemas revisará en forma periódica la base de datos de cuentas de usuarios existentes, y generará un listado de aquéllas que no registren uso en tres meses con el fin de analizar y evaluar la posibilidad de su baja (con base en la revisión periódica de cuentas de usuario.

30. En las sucursales, Unidades Operativas y Almacenes, el enlace informático de la localidad será el responsable de configurar los accesos en los equipos de cómputo de las personas usuarias de su adscripción (incluyendo almacenes bajo su responsabilidad), asimismo será el responsable de proporcionar a sus personas usuarias el soporte técnico de primer nivel, llevar el registro de las cuentas de su adscripción, y notificar cualquier actualización (alta, baja o cambio) a la Gerencia de Sistemas mediante un reporte generado a través de la mesa de servicio.

31. Respecto a la configuración y establecimiento de contraseñas de cuentas de usuarios del directorio activo, el detalle se define en el documento independiente llamado "Guía para cambio de contraseñas", el cual se encuentra disponible en la Intranet de Diconsa, S.A. de C.V.

32. Alta de personas usuarias

- En Oficinas Centrales, las personas titulares de las áreas como: Dirección General, Dirección de Área o Gerencias, podrán solicitar a la Gerencia de Sistemas mediante oficio, tarjeta o a través de la herramienta de gestión de la mesa de servicio que se proporcionen o cancelen servicios al personal bajo su mando.

33. Baja/Cancelación de personas usuarias

- En caso de que la persona usuaria tenga problemas relacionados con su cuenta, deberá reportarlos a la Gerencia de Sistemas, a través de la mesa de servicio de Diconsa, S.A. de C.V., donde se registrará un incidente para ser atendido por soporte técnico.
- La Gerencia de Sistema aplicará la baja o cancelación de cuentas de usuarios y de correo electrónico de personal que ya no labore en Diconsa, S.A. de C.V. cuando:

➢ La Gerencia de Recursos Humanos enviará en archivo electrónico a la Gerencia de Sistemas, con los movimientos efectivos de BAJAS de personal en la Entidad a nivel nacional (esto lo realizará al menos una vez al mes).

➢ Las Sucursales y Unidades Operativas a través de los enlaces informáticos que soliciten ante la mesa de servicio de Diconsa, S.A. de C.V., la baja de cuentas de usuarios que ya no laboran en la Entidad.

➢ En Oficinas Centrales, las personas titulares de las áreas como: Director(a) General, Director(a) o Gerente(a) soliciten por escrito la baja y/o cancelación de los usuarios (as) que ya no laboran en la Entidad

- Si las bajas no son notificadas por ninguno de los tres métodos anteriores, la Gerencia de Sistemas NO se hará responsable de la aplicación de las mismas.
- La única excepción a lo anterior se presentará, cuando por la revisión técnica efectuada por la Gerencia de Sistemas, se detecten cuentas de usuarios que no hayan sido utilizadas en un periodo de tres meses desde su último acceso; en cuyo caso dichas cuentas serán eliminadas del directorio activo.
- La Gerencia de Sistemas sólo podrá cancelar o dar de baja un acceso sin previa solicitud externa, cuando se presenten aquellos casos extraordinarios donde el acceso de un usuario con dicha cuenta represente un riesgo de seguridad para la Entidad. O bien, podrá inhabilitar una cuenta (sin eliminarla), siempre y cuando tenga conocimiento de que la misma ya no se utiliza.

34. Protección de Contraseñas

- Las contraseñas son intransferibles y personales y no deben de ser compartidas. Todas las contraseñas deben ser tratadas como sensibles, como Información confidencial de Diconsa, S.A. de C.V.
- Las contraseñas no se deben adjuntar en mensajes de correo electrónico u otras formas de comunicación electrónica.
- Las contraseñas no deben ser reveladas por teléfono a nadie.
- No se deben de revelar contraseñas en cuestionarios o formularios de seguridad o de ningún tipo.
- No deben dejarse pistas del formato de una contraseña (por ejemplo, nombre de mi familia).
- No se deberán compartir contraseñas de Diconsa, S.A. de C.V. con nadie, incluyendo asistentes, administrativos, secretarias, compañeros de trabajo, amigos o miembros de la familia durante las vacaciones o cuando se esté trabajando desde casa.
- No se deberán escribir ni guardar contraseñas en post-its o papel en cualquier lugar de su oficina.
- No se deberán guardar las contraseñas en los archivos de las computadora o dispositivos móviles (teléfonos, tabletas) sin cifrado.
- No se deberá utilizar la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web)
- Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar todas sus contraseñas a la brevedad.

35. Restricciones complementarias:

- Está prohibido que cualquier persona ajena a Diconsa, S.A. de C.V. haga uso del acceso a Internet salvo autorización expresa de la Gerencia de Sistemas.
- El uso de dispositivos de Internet móvil (BAM, banda ancha) propios queda absolutamente prohibido en computadoras que pertenezcan a Diconsa, S.A. de C.V., salvo autorización expresa de la Gerencia de Sistemas.
- No duplicar software licenciado o con derechos de autor a menos que se especifique explícitamente que está permitido.
- No deberá usarse el Internet para realizar llamadas Internacionales (Oialpad, NET2Phone, FreePhone, etc.).
- Está estrictamente prohibido la copia no autorizada de materiales con derechos de autor, incluyendo, pero no limitado a la digitalización y distribución de fotografías de revistas, libros u otras fuentes con derechos de autor, la música con derechos de autor y la instalación de software con derechos de autor para el cual la empresa o el/la usuario(a) final no cuenta con una licencia activa.
- Está prohibido el acceso a datos, servidores o cuentas para cualquier propósito que no sea para la realización de actividades de sus funciones.
- La exportación de software, información técnica, software o tecnología de cifrado, en violación de las leyes internacionales o regionales de control de exportaciones, es ilegal. El usuario deberá consultar a través de la mesa de servicio el manejo adecuado antes de

la exportación de cualquier material de esta índole.

- Está prohibido la Introducción de programas maliciosos en la red o en servidores (por ejemplo, virus, gusanos, caballos de Troya, bombas de correo electrónico, etc.).
- El uso de un activo de cómputo de la empresa para participar, reclutar o transmitir materiales que están en violación de las leyes locales de acoso sexual u hostilidad en el lugar de trabajo.
- Hacer ofertas fraudulentas de productos, artículos o servicios procedentes de cualquier cuenta propiedad de la empresa.
- Efectuar brechas de seguridad o interrupciones de la comunicación en red. Las violaciones de seguridad incluyen, pero no se limitan a acceder a datos para los que no se es destinatario o conectarse a un servidor o cuenta a la cual la persona no está expresamente autorizada a acceder, a menos que estas funciones estén dentro del alcance de sus funciones regulares. Para los propósitos de esta sección, "interrupción" incluye, pero no se limita al espionaje en la red, inundaciones de ping, suplantación de paquetes, denegación de servicios, etc., con fines maliciosos.
- El Escaneo de Puertos y escaneos de seguridad están expresamente prohibidos a menos que se realice una notificación y autorización previa ante el departamento de la Gerencia de Sistemas.
- Eludir la autenticación de usuarios(as) y la seguridad de cualquier equipo de cómputo, de red o cuenta.
- El uso de cualquier programa / script / comando o el envío de mensajes de cualquier tipo, con la intención de interferir o deshabilitar las sesiones de terminal de algún usuario, a través de cualquier medio, de forma local o a través de Internet / Intranet / Extranet.
- Proporcionar información sobre empleados(as) o listas de los/las empleados(as) de la empresa a externos.
- La extracción de información propiedad de Diconsa, S.A. de C.V. utilizando cualquier medio que no esté relacionada con sus labores normales de trabajo.

VIII. PROCEDIMIENTOS

1. Procedimiento para solicitar la creación el desarrollo de un sistema.
2. Procedimiento para solicitar cuentas de usuario/correo electrónico.
3. Procedimiento para la solicitud de activos de Tecnología.
4. Procedimiento para el reporte de fallas, requerimientos y solicitudes.
5. Procedimiento para la solicitud de envío y recepción de correos de dominios públicos gratuitos.
6. Procedimiento para la solicitud de acceso vía remota VPN.
7. Procedimiento para la solicitud de respaldo de información.
8. Procedimiento para el Monitoreo de uso de Internet.
9. Procedimiento para la validación de cuentas de usuario.
10. Procedimiento en caso de robo, daño o siniestro.

VIII.1 PROCEDIMIENTO PARA SOLICITAR LA CREACIÓN DEL DESARROLLO DE UN SISTEMA

OBJETIVO GENERAL

Promover la práctica y uso de la metodología de desarrollo de sistemas, estandarizando de forma transversal para Diconsa, S.A. de C.V., el proceso de cómo documentar y dar seguimiento a los proyectos de desarrollo de sistemas de una manera ágil y eficiente, proporcionando las herramientas necesarias, así como describiendo de manera clara el ciclo de vida del proyecto y los entregables que podrían ser ocupados a través de los diferentes procesos, los cuales conforman el marco de la metodología a implementar.

OBJETIVO ESPECÍFICO

Describir el orden de las actividades necesarias para que las personas servidoras públicas de Diconsa, S.A. de C.V., soliciten a la Gerencia de Sistemas desarrollar un sistema de una manera ágil y eficiente.

POLÍTICAS DE OPERACIÓN

1. El área solicitante a través del superior jerárquico con cargo mínimo de subgerente solicitará el desarrollo de un sistema, donde justifique y/o indique los motivos que sus actividades requieran lo solicitado, mediante la entrega del formato "ACTA DE CONSTITUCIÓN DEL PROYECTO/REQUERIMIENTO DEL USUARIO" (**Anexo 1**)
2. El superior jerárquico deberá remitir la autorización de la implementación del sistema otorgada al usuario y solicitar a la Subgerencia de Desarrollo de Sistemas adscrita a la Gerencia de Sistemas, vía oficio, correo electrónico y/o nota informativa la creación del sistema, para poder desempeñar sus actividades designadas.
3. La Subgerencia de Desarrollo de Sistemas, a través de la Mesa de Servicio, recibirá y dará trámite a la solicitud de creación del desarrollo del sistema, realizada mediante oficio por el superior jerárquico del área solicitante.
4. La Subgerencia de Desarrollo de Sistemas, realizará la planificación, es decir, define al equipo de trabajo y crea una hoja de ruta del proyecto.
5. El equipo de trabajo realiza un cronograma por sprints/road map, el cual permite identificar la ruta que seguirá el proyecto, en el cual se identifica la duración, sprints de entrega e hitos de control.
6. El equipo de trabajo realiza el kick off, el cual permite dar el inicio formal de las actividades planificadas, detallando hitos importantes del proyecto, comités de seguimiento, riesgos y siguientes pasos.
7. La Subgerencia de Desarrollo de Sistemas realiza el seguimiento y control, es decir, entrega el valor al área solicitante, esta fase contempla el desarrollo, pruebas unitarias, casos de pruebas, matriz de pruebas, pruebas integrales, reuniones de seguimiento, capacitación y liberación de cada uno de los sprints planificados, pudiendo existir controles de cambios en esta fase los cuales tendrían que ser planificados en un nuevo sprint.
8. La Subgerencia de Desarrollo de Sistemas remite un reporte de avances, en el cual indica el estatus actual del proyecto de manera resumida, riesgos, problemas y los pasos siguientes.

9. La Subgerencia de Desarrollo de Sistemas remite la matriz de pruebas, la cual permite demostrar al área solicitante que el desarrollo satisface el requerimiento y es factible liberar el desarrollo en un ambiente productivo.

10. La Gerencia de Sistemas, a través de la Subgerencia de Desarrollo de Sistemas, convocan a capacitación, al personal que operará el sistema desarrollado.

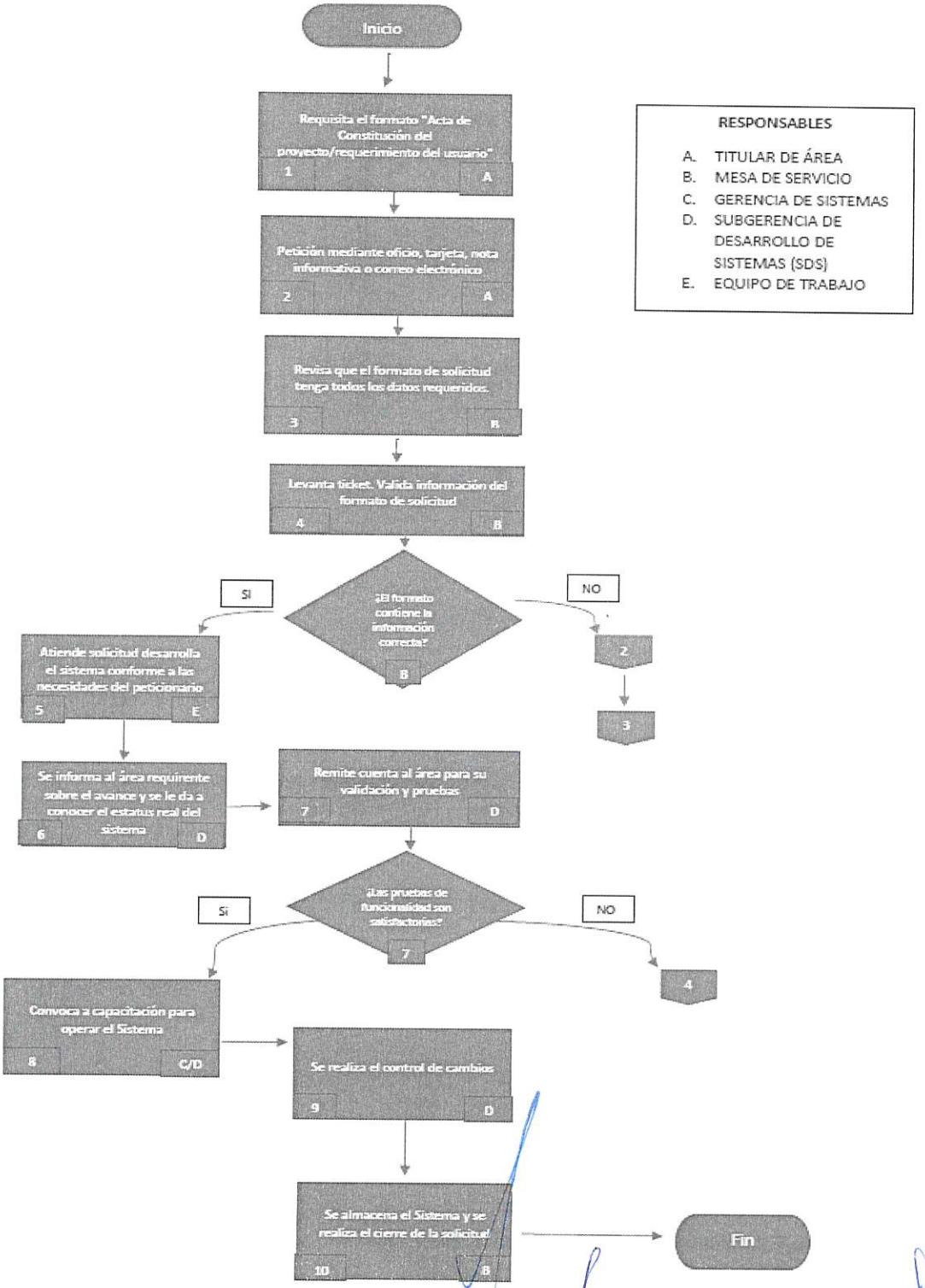
11. Una vez realizada la capacitación, se realiza el control de cambios, el cual permite justificar el desarrollo de una nueva funcionalidad diferente o adicional al requerimiento original, el cual comprende la solicitud de cambio, evaluación, aprobación o rechazo e implementación del mismo. (**Anexo 2**)

12. Por último, en el cierre, se formaliza que se han alcanzado los objetivos planteados de un entregable o proyecto, los cuales han sido debidamente aprobados. (**Anexo 3**)

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	El área solicitante	Descarga formato "Acta de Constitución del proyecto/requerimiento del usuario"	"Acta de Constitución del proyecto/requerimiento del usuario"
2	El área solicitante	Petición por parte de la persona Titular de Área mediante Oficio, Tarjeta, Nota Informativa o correo electrónico enviando el formato firmado.	
3	Mesa de Servicio	Revisa formato de solicitud si presenta todos los datos requeridos manteniendo comunicación con el área solicitante.	"Acta de Constitución del proyecto/requerimiento del usuario"
4	Mesa de Servicio	Levanta ticket. Valida información del formato de solicitud. ¿Formato contiene información correcta? Sí, ir al paso 5 No, ir al paso 2 y 3.	"Acta de Constitución del proyecto/requerimiento del usuario" Ticket
5	Equipo de Trabajo Asignado	Atiende la solicitud, desarrolla el sistema y se encarga de que cumpla con las necesidades solicitadas por el área peticionaria.	"Acta de Constitución del proyecto/requerimiento del usuario"
6	Subgerencia de Desarrollo de Sistemas	Se informa al área requirente sobre el avance y se le da a conocer el estatus real del sistema.	
7	Subgerencia de Desarrollo de Sistemas	Remite cuenta (s) al solicitante para su validación y pruebas. ¿Las pruebas de funcionalidad son satisfactorias? No, ir al paso 4 Si, ir al paso 8	
8	Gerencia de Sistemas/Subgerencia de Desarrollo de Sistemas	Convocan a capacitación del personal que operará dicho sistema.	
9	Subgerencia de Desarrollo de Sistemas	Se realiza el control de cambios. ¿Cumple con los objetivos planteados? No, ir al paso 4 Si, ir al paso 10	
10	Mesa de Servicio	Almacena el Sistema en su plataforma	
		Fin del Procedimiento	

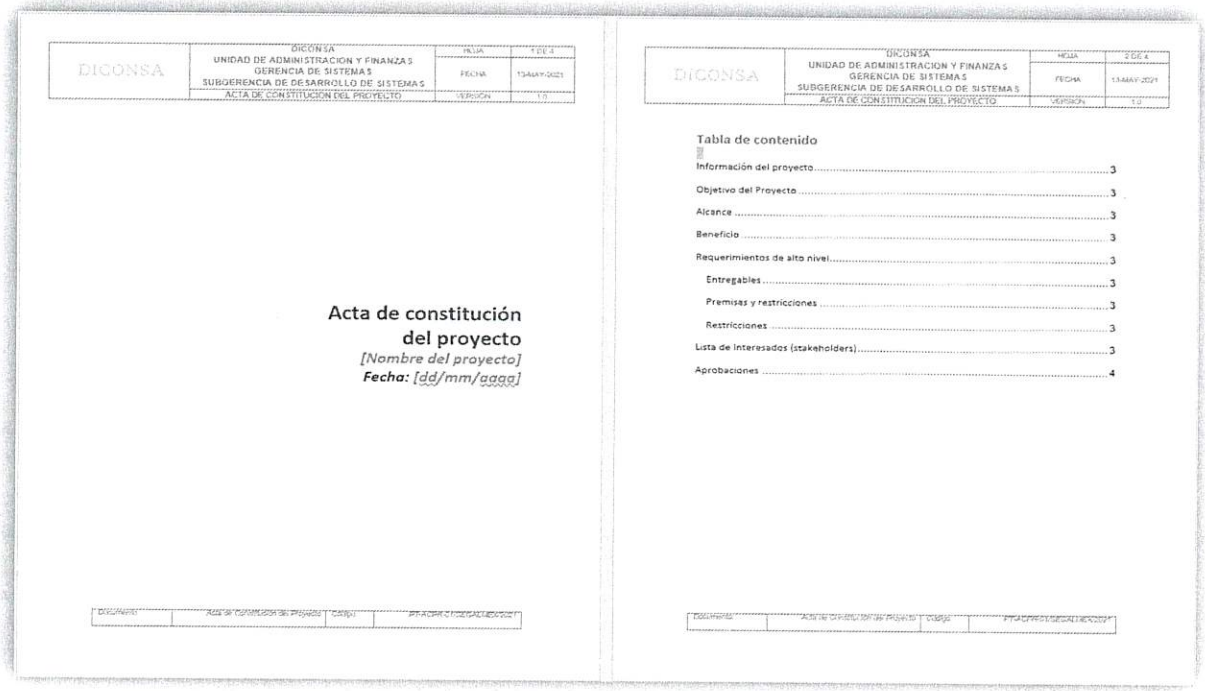
DIAGRAMA DE FLUJO



RELACIÓN DE ANEXOS

Número	Nombre del Documento	Clave
1	"Acta de Constitución del proyecto/requerimiento del usuario"	
2	"Solicitud de cambio"	
3	"Acta de cierre de Proyecto"	

ANEXO 1
"ACTA DE CONSTITUCIÓN DEL PROYECTO/REQUERIMIENTO DEL USUARIO"

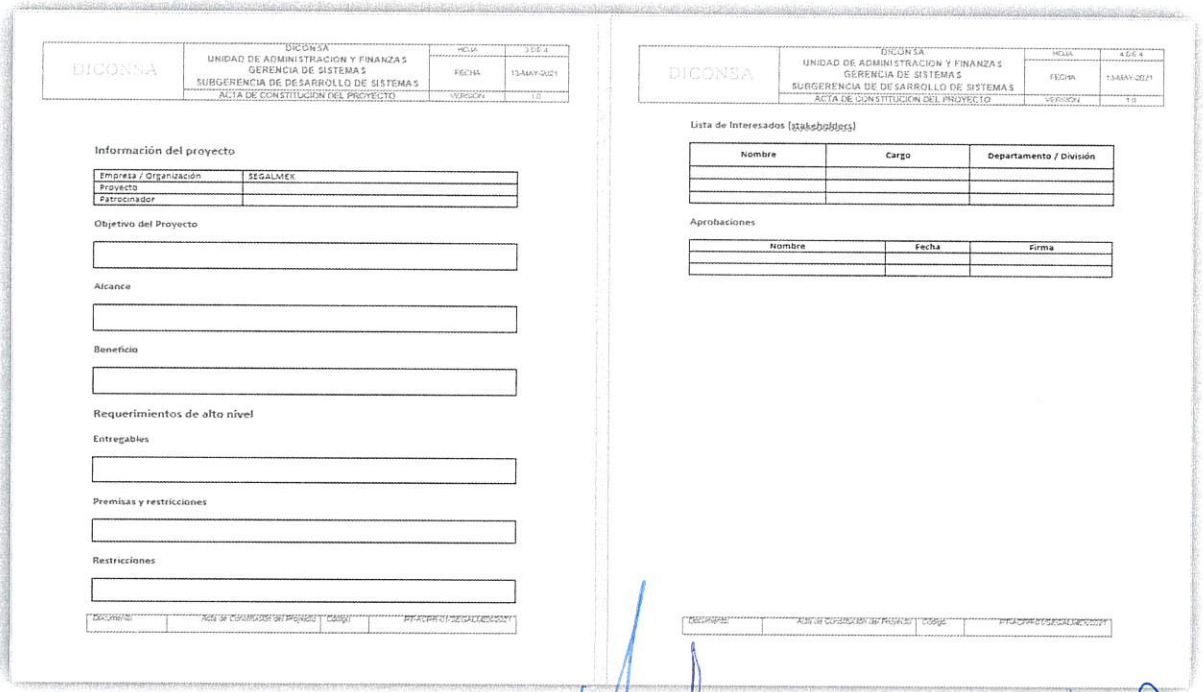


DICONSA
UNIDAD DE ADMINISTRACION Y FINANZAS
GERENCIA DE SISTEMAS
SUBGERENCIA DE DESARROLLO DE SISTEMAS
ACTA DE CONSTITUCION DEL PROYECTO
HOJA 1 DE 4 | FECHA 13-MAY-2021 | VERSIÓN 1.0

Acta de constitución del proyecto
[Nombre del proyecto]
Fecha: *[dd/mm/aaaa]*

DICONSA
UNIDAD DE ADMINISTRACION Y FINANZAS
GERENCIA DE SISTEMAS
SUBGERENCIA DE DESARROLLO DE SISTEMAS
ACTA DE CONSTITUCION DEL PROYECTO
HOJA 2 DE 4 | FECHA 13-MAY-2021 | VERSIÓN 1.0

Tabla de contenido



DICONSA
UNIDAD DE ADMINISTRACION Y FINANZAS
GERENCIA DE SISTEMAS
SUBGERENCIA DE DESARROLLO DE SISTEMAS
ACTA DE CONSTITUCION DEL PROYECTO
HOJA 3 DE 4 | FECHA 13-MAY-2021 | VERSIÓN 1.0

Información del proyecto

Empresa / Organización	SEGALMEX
Proyecto	
Patrocinador	

Objetivo del Proyecto

Alcance

Beneficio

Requerimientos de alto nivel

Entregables

Premisas y restricciones

Restricciones

DICONSA
UNIDAD DE ADMINISTRACION Y FINANZAS
GERENCIA DE SISTEMAS
SUBGERENCIA DE DESARROLLO DE SISTEMAS
ACTA DE CONSTITUCION DEL PROYECTO
HOJA 4 DE 4 | FECHA 13-MAY-2021 | VERSIÓN 1.0

Lista de Interesados (stakeholders)

Nombre	Cargo	Departamento / División

Aprobaciones

Nombre	Fecha	Firma

ANEXO 2
"SOLICITUD DE CAMBIO"

DICONSA	DICONSA UNIDAD DE ADMINISTRACIÓN Y FINANZAS GERENCIA DE SISTEMAS SUBGERENCIA DE DESARROLLO DE SISTEMAS	ID Solicitud Fecha DD/MM/AAAA
	SOLICITUD DE CAMBIO	Versión 1

I. Origen de la Solicitud de Cambio.

Título del Cambio:		Aplicación Tía cambiar	
Nombre del Solicitante:			
Área de adscripción:		Teléfono y extensión:	

II. Tipo de la Solicitud de Cambio

Descripción del Cambio

Beneficio					
Bajo		Medio		Alto	
Especifique los motivos:					

PARA LLENAR POR PARTE DE ÁREA RESOLUTORA

I. Análisis del Impacto.

Áreas Involucradas					
Sistemas		Comunicaciones		Infraestructura	
Base de Datos		Seguridad			

Sistemas involucrados											
SIPRESA		SAP		SIACCION		PIRAMO		SIPLATAMA		SIAP	
MOPAC		SAP		SICKO		SINTRA2		SICDOM		CAEN	
SIAC		BiControl		Red e Internet		PROVEEDORES		COMPENDIO		SIPAR	

Riesgo					
Bajo		Medio		Alto	
Indicar riesgos:					

Fecha de Entrega	DD/MM/AAAA

Nombre y firma del solicitante

Nombre y firma de quien autoriza

Cláusula de propiedad y confidencialidad
La información contenida en este formato está clasificada como confidencial. Es proporcionada al Grupo de Cambios y demás participantes con la restricción de no ser divulgada. 1 de 1

ANEXO 3
"ACTA DE CIERRE DE PROYECTO"

DICONSA	DICONSA UNIDAD DE ADMINISTRACION Y FINANZAS GERENCIA DE SISTEMAS SUBGERENCIA DE DESARROLLO DE SISTEMAS	[illegible]	[illegible]
		FECHA	DD/MM/AAAA
	ACTA DE CIERRE DE PROYECTO	VERSIÓN	1.0

Proyecto:			
Fecha Inicio del Proyecto:		Fecha Fin del Proyecto:	
Elaborado por:			
Lugar y Fecha:			

Objetivo

Formalizar el cierre del proyecto	

Actividades realizadas

Se formaliza la finalización y cierre del proyecto de acuerdo al alcance especificado.

Servicio	Estatus
	Realizado

Documentación Entregada

Observaciones

Los trabajos listados como adicionales anteriormente no impactan costo adicional al proyecto, únicamente son de manera informativa.

El punto de contacto para el soporte de cualquier incidente será mediante la mesa de ayuda por medio del correo electrónico sop_segalmex@segalmex.gob.mx.

De acuerdo a los trabajos realizados, se aprueba por todas las partes involucradas que los servicios desarrollados han quedado debidamente ejecutados y finalizados.

No habiendo más asuntos que tratar, se levantó la presente acta, firmando al calce todos los que intervinieron.

Área Usuaria (COLOCAR NOMBRE DE LA SUBGERENCIA)

NOMBRE	PUESTO	FECHA	FIRMA

SUBGERENCIA DE DESARROLLO DE SISTEMAS

NOMBRE	PUESTO	FECHA	FIRMA

[illegible]	[illegible]	[illegible]	[illegible]

VIII.2 PROCEDIMIENTO PARA SOLICITAR CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO

OBJETIVO

Describir el orden de las actividades necesarias para que las áreas de Diconsa, S.A. de C.V., soliciten a la Gerencia de Sistemas cuentas de usuario(a)/correo electrónico institucional.

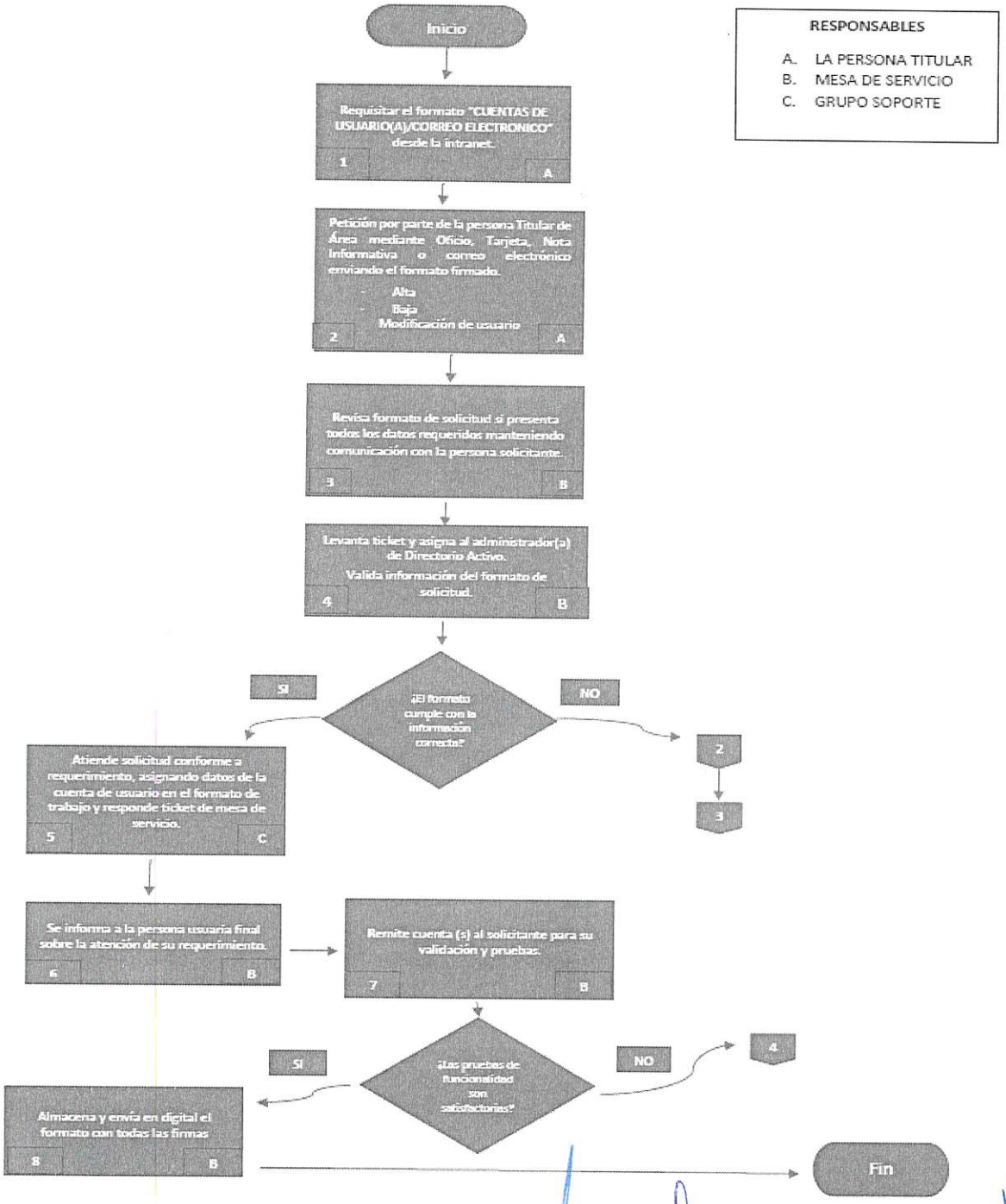
POLÍTICAS DE OPERACIÓN

1. El área solicitante a través del superior jerárquico con cargo mínimo de subgerencia solicitará la asignación de una cuenta de usuario y correo electrónico, donde indique los motivos que sus actividades requieran del acceso a los recursos informáticos mediante la entrega del formato "CUENTAS DE USUARIO(A)/CORREO ELECTRONICO " (**Anexo 1**).
2. El superior jerárquico de la persona usuaria deberá remitir la autorización y solicitar a la Gerencia de Sistemas, vía oficio, correo electrónico y/o nota informativa la asignación de la cuenta de usuario y correo electrónico.
3. La Subgerencia de Infraestructura y Telecomunicaciones a través de la Mesa de Servicio, recibirá y dará trámite a la solicitud de cuenta de usuario/correo electrónico.
4. La dirección electrónica que se crea será asignada tanto para el correo electrónico como para el directorio activo.
5. Una vez atendido el reporte, la persona usuaria recibirá un correo de validación de la atención del servicio, el cual deberá contestar para que se lleve a cabo el cierre de ticket o número de reporte.
6. El administrador otorgará cuenta de acceso a las personas usuarias previa autorización y solicitud de su área de adscripción.
7. El área solicitante deberá verificar que los permisos solicitados no violen la segregación de funciones, así como que los permisos sean los mínimos necesarios para que el usuario realice sus funciones.
8. El administrador otorgará sólo los niveles de permisos mínimos necesarios para que cada usuario pueda realizar sus actividades cotidianas.
9. Cada cuenta deberá implementar la política de modificación de claves de acceso (password) de forma periódica y obligada.
10. La clave de acceso asignada a cada persona usuaria deberá estar formada por letras, números y símbolos con una longitud mínima de 8 caracteres

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	La persona Titular de área con ayuda de La persona Enlace Informático	Descargar el formato "CUENTAS DE USUARIO(A)/CORREO ELECTRONICO" desde la intranet.	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO"
2	La persona Titular de área con ayuda de La persona Enlace Informático	Petición por parte de la persona Titular de Área mediante Oficio, Tarjeta, Nota Informativa o correo electrónico enviando el formato firmado. · Alta · Baja · Modificación de usuario	"OFICIO, TARJETA, NOTA INFORMATIVA O CORREO ELECTRÓNICO"
3	Mesa de Servicio	Revisa formato de solicitud si presenta todos los datos requeridos manteniendo comunicación con la persona solicitante.	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO"
4	Mesa de Servicio	Levanta ticket y asigna al administrador(a) de Directorio Activo. Valida información del formato de solicitud. ¿Formato contiene información correcta? Sí, ir al paso 5. No, ir al paso 2 y 3.	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO" Ticket
5	La persona Administradora de Directorio Activo y correo electrónico	Atiende solicitud conforme a requerimiento, asignando datos de la cuenta de usuario en el formato de trabajo y responde ticket de mesa de servicio.	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO"
6	Mesa de Servicio	Se informa a la persona usuaria final sobre la atención de su requerimiento.	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO"
7	Mesa de Servicio	Remite cuenta (s) al solicitante para su validación y pruebas. ¿Las pruebas de funcionalidad son satisfactorias? No, ir al paso 4 Si, ir al paso 8	
8	Mesa de Servicio	Almacena y envía en digital el formato con todas las firmas	
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



RELACIÓN DE ANEXOS

Número	Nombre del Documento	Clave
1	"CUENTAS DE USUARIO(A)/CORREO ELECTRÓNICO"	

ANEXO 1
"CUENTAS DE USUARIO(A)/CORREO ELECTRONICO"

SEGALMEX DICONSA | LICONSA	SEGALMEX, DICONSA Y LICONSA UNIDAD DE ADMINISTRACION Y FINANZAS GERENCIA DE SISTEMAS SUBGERENCIA DE INFRAESTRUCTURA Y TELECOMUNICACIONES	HOJA	1 DE 1
		PROCESO	AOP
		VER. 1.0	2022
	CUENTAS DE USUARIO/CORREO ELECTRONICO		

								Fecha Solicitud:			
Solicitud de Cuenta											
Usuario de Dominio					Correo Electrónico						
Dominio	@segalmex.gob.mx			@diconsa.gob.mx			@liconsa.gob.mx				

Datos Usuario	
Nombre:	
Apellido Paterno:	
Apellido Materno:	
Cargo:	
Área de Adscripción:	
Cuenta de Correo:	
No. Telefónico:	No. de Extensión:

Datos de la unidad Solicitante	
Unidad Responsable:	
Área:	
Jefe Inmediato que Autoriza:	
Puesto	

Tipo de Movimiento											
Alta				Baja				Cambio			

Políticas de aceptación de usuario

- El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada.
- La cuenta es para uso personal e intransferible Es responsabilidad de cada usuario el resguardo y seguridad del nombre de usuario y contraseña
- Es responsabilidad del área que solicita el alta de un usuario, solicitar la baja del usuario
- No compartir la cuenta de usuario con otras personas
- Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada sólo después de haber tomado las medidas necesarias a consideración de la Gerencia de Sistemas
- El usuario acepta que la contraseña deberá ser cambiada al menos cada 3 meses
- La longitud de la contraseña debe ser al menos de 8 caracteres y contener caracteres tanto en mayúsculas como en minúsculas
- El usuario acepta y acatara en todo momento las Políticas contenidas en la Guía para el Uso del Correo Electrónico y Guía para el Uso del Servicio de Internet publicados en la Intranet de la Entidad

Autorizo Unidad Solicitante	Usuario	Autorizo Subgerencia de Infraestructura y Telecomunicaciones
Nombre y Firma	Nombre y Firma	Nombre y Firma

Favor de enviar este formato debidamente llenado y firmado a la brevedad a la Gerencia de Sistemas y con la finalidad de agilizar el trámite levantar el ticket en la mesa de ayuda adjuntando este formato firmado en formato PDF

VIII.3 PROCEDIMIENTO PARA LA SOLICITUD DE ACTIVOS DE TECNOLOGÍA

OBJETIVO

Describir el orden de las actividades necesarias para que las personas servidoras públicas de Diconsa, S.A. de C.V. soliciten a la Gerencia de Sistemas la asignación y resguardo de activos de Tecnología.

POLÍTICAS DE OPERACIÓN

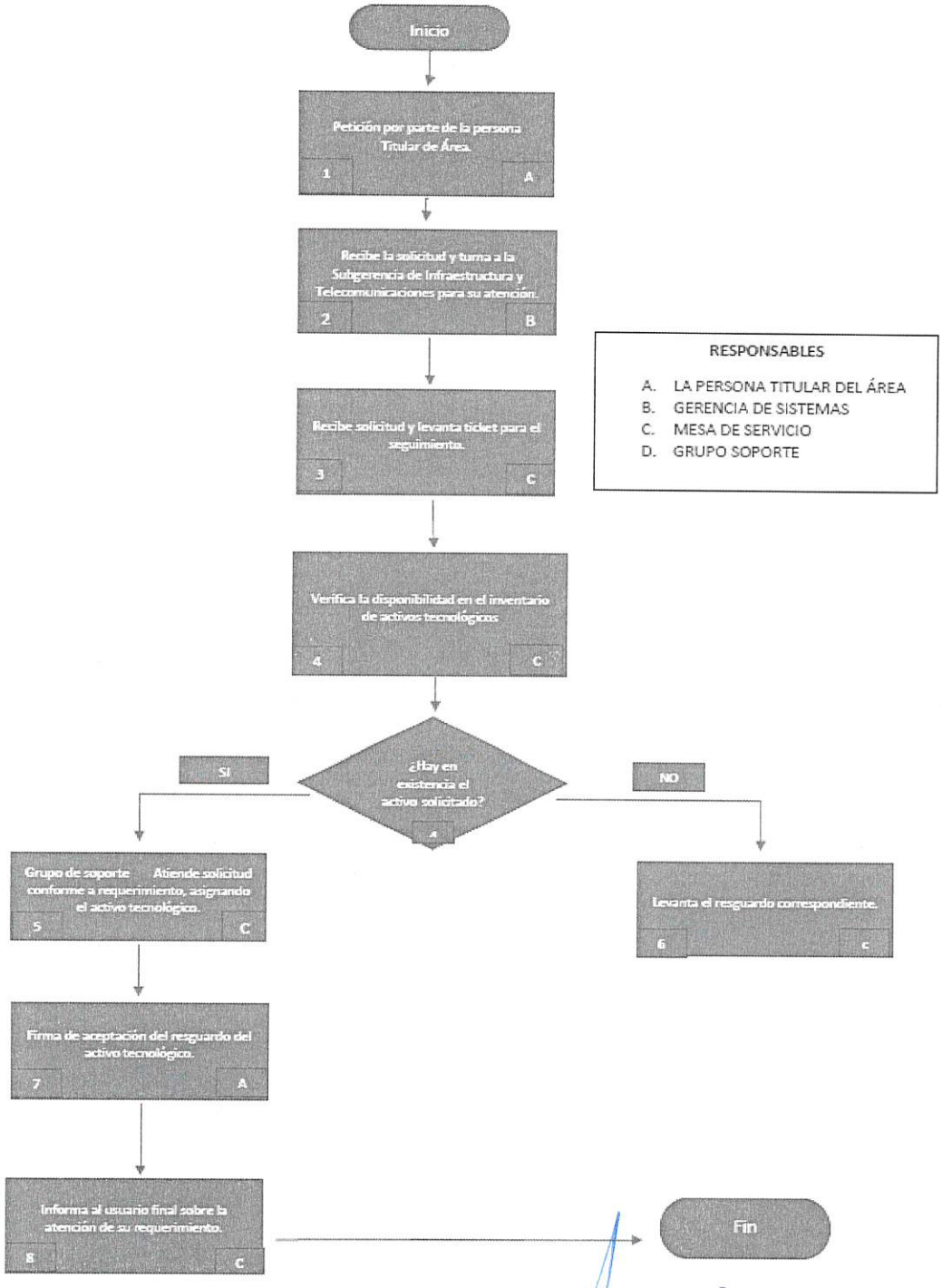
1. La persona usuaria deberá solicitar a su superior jerárquico la autorización para la asignación o préstamo de activos de tecnología, en el que indique los motivos que sus actividades requieran para dicha asignación o préstamo.
2. El superior jerárquico de la persona usuaria deberá remitir la autorización y solicitar a la Gerencia de Sistemas, vía oficio, correo electrónico y/o nota informativa la asignación de activos de tecnología.
3. La Subgerencia de Infraestructura y Telecomunicaciones a través de la Mesa de Servicio, recibirá y dará trámite a la solicitud de asignación de activos de tecnología.
4. La Subgerencia de Infraestructura y Telecomunicaciones valorara de acuerdo con su inventario la factibilidad de la asignación del activo solicitado.
5. Una vez asignado el activo tecnológico, el usuario será el responsable del uso, manejo y resguardo correspondiente.
6. Datos requeridos por parte del usuario para la asignación del activo:

Datos del Usuario	
Solicitud o Falla:	
Usuario Resguardante:	
Correo:	
N° de Empleado	
Centro de Trabajo:	
Dirección o Ubicación:	
Piso:	
Adscripción:	
Área o Departamento:	
Cargo o Puesto:	
Teléfono:	
Extensión:	
Horario en que se encuentra al usuario:	
Usuario Final:	

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	La persona usuaria Titular de área	Petición por parte de la persona Titular de Área.	Oficio, Tarjeta, Nota Informativa o correo electrónico
2	Gerencia de Sistemas	Recibe la solicitud y turna a la Subgerencia de Infraestructura y Telecomunicaciones para su atención.	
3	Mesa de Servicio	Recibe solicitud y levanta ticket para el seguimiento.	Ticket
4	Grupo de soporte	Verifica la disponibilidad en el inventario de activos tecnológicos ¿Hay en existencia el activo solicitado? Sí, ir al paso 5 No, ir al paso 6	
5	Grupo de soporte	Atiende solicitud conforme a requerimiento, asignando el activo tecnológico.	Resguardo
6	Grupo de soporte	Levanta el resguardo correspondiente.	
7	Persona usuaria del equipo o persona Titular de área	Firma de aceptación del resguardo del activo tecnológico.	
8	Mesa de Servicio	Informa al usuario final sobre la atención de su requerimiento.	Correo electrónico
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



VIII.4 PROCEDIMIENTO PARA EL REPORTE DE FALLAS, REQUERIMIENTOS Y SOLICITUDES

OBJETIVO

Describir el orden de las actividades necesarias para que las personas servidoras públicas de Diconsa, S.A. de C.V. lleven a cabo el reporte de fallas, requerimientos y solicitudes.

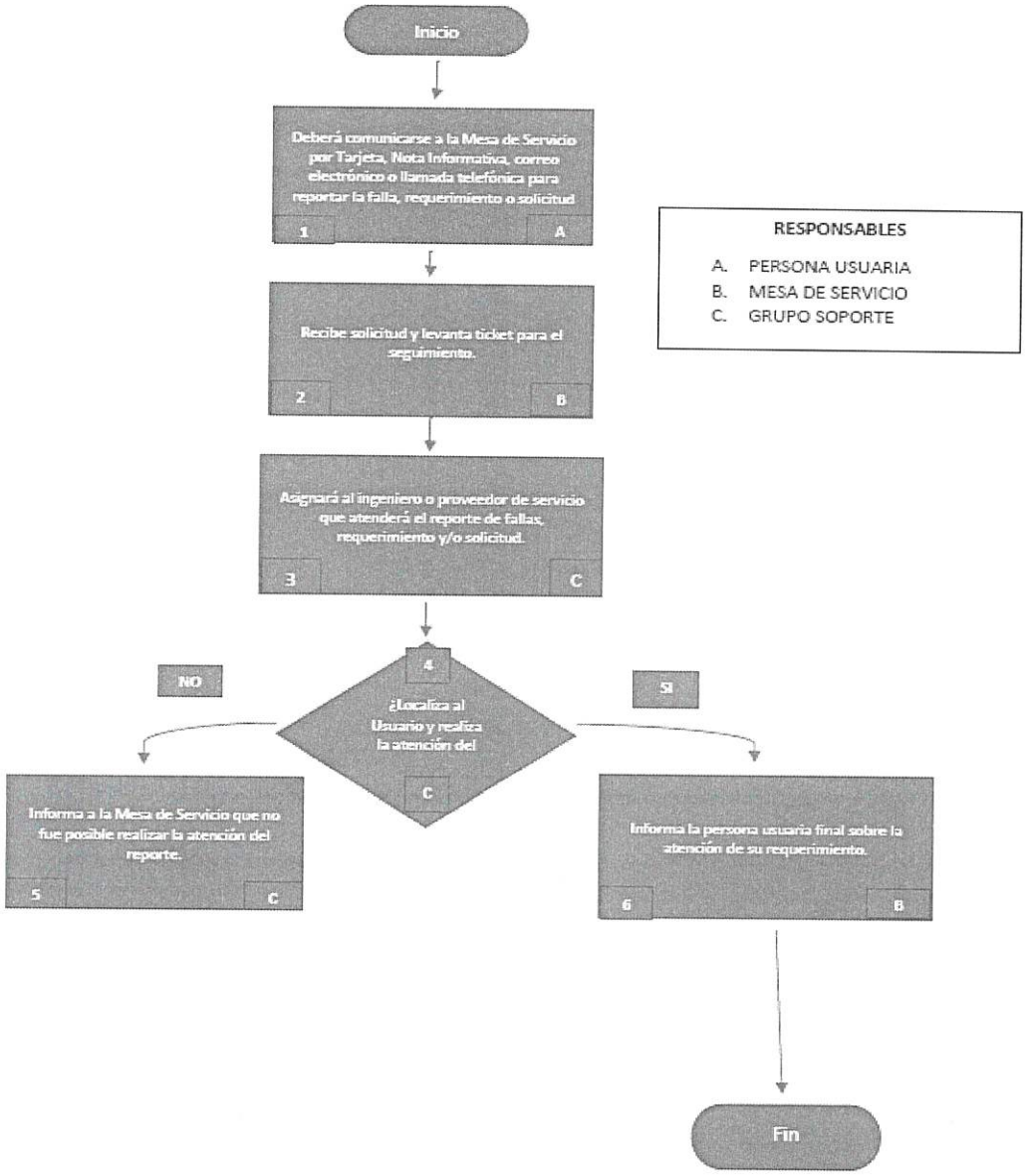
POLÍTICAS DE OPERACIÓN

1. La persona usuaria deberá reportar las fallas, requerimientos y solicitudes en materia de tecnologías de la información, a la Mesa de Servicio de Diconsa, S.A. de C.V., le asignará un número de reporte, que servirá para dar seguimiento al mismo.
2. La persona usuaria, preferentemente deberá otorgar las facilidades necesarias para que el personal de la Gerencia de Sistemas realice su labor. En caso de que el usuario, no pueda atender al ingeniero de servicio, este deberá de dirigirse al superior jerárquico del usuario con la finalidad de atender el reporte.
3. Si el personal de la Gerencia de Sistemas no pudiera realizar su labor por no encontrar al usuario, este informará a la Mesa de Servicio para que se informe al usuario que no fue posible localizarlo, si al tercer intento no se localiza al usuario, el reporte se dará por atendido.
4. Una vez atendido el reporte, la persona usuaria recibirá un correo de validación de la atención del servicio, el cual deberá contestar para que se lleve a cabo el cierre de número de reporte.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Persona usuaria	Deberá comunicarse a la Mesa de Servicio por Tarjeta, Nota Informativa, correo electrónico o llamada telefónica para reportar la falla, requerimiento o solicitud.	Tarjeta, Nota Informativa o correo electrónico
2	Mesa de Servicio	Recibe solicitud y levanta ticket para el seguimiento.	Ticket
3	Grupo de soporte	Asignará al personal de la Gerencia de Sistemas o proveedor de servicio que atenderá el reporte de fallas, requerimiento y/o solicitud.	
4	Grupo de soporte	¿Localiza al Usuario y realiza la atención del reporte? Sí, ir al paso 6 No, ir al paso 5	
5	Grupo de soporte	Informa a la Mesa de Servicio que no fue posible realizar la atención del reporte.	
6	Mesa de Servicio	Informa la persona usuaria final sobre la atención de su requerimiento.	Correo electrónico
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



VIII.5 PROCEDIMIENTO PARA LA SOLICITUD DE ENVÍO Y RECEPCIÓN DE CORREOS DE DOMINIOS PÚBLICOS GRATUITOS

OBJETIVO

Describir el orden de las actividades necesarias para que las personas servidoras públicas de Diconsa, S.A. de C.V. obtengan los permisos para el envío y recepción de correos de dominios públicos.

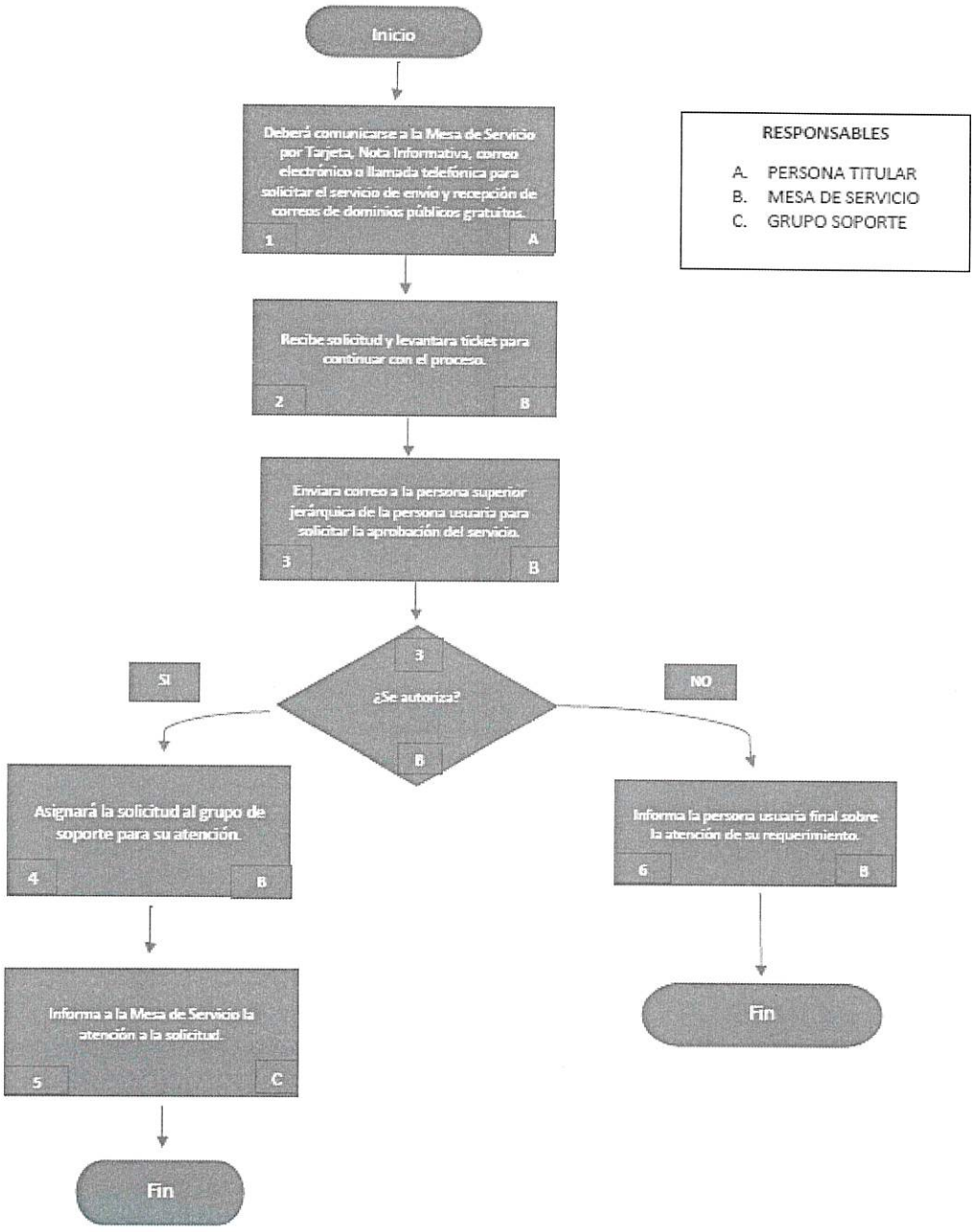
POLÍTICAS DE OPERACIÓN

1. La Gerencia de Sistemas será la única que podrá autorizar el envío y recepción de correos de dominios públicos.
2. El superior jerárquico o la persona usuaria deberán justificar que para la realización de sus funciones o actividades es necesario contar con el servicio de envío y recepción de correos de dominios públicos.
3. El servicio deberá utilizarse exclusivamente para atender asuntos inherentes a la entidad.
4. El usuario será el único responsable del uso del servicio.
5. La Gerencia de Sistemas en cualquier momento podrá suspender el servicio si detecta un uso inadecuado que violente la seguridad de la entidad.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Persona Titular de área o persona usuaria	Deberá comunicarse a la Mesa de Servicio por Tarjeta, Nota Informativa, correo electrónico o llamada telefónica para solicitar el servicio de envío y recepción de correos de dominios públicos gratuitos.	Tarjeta, Nota Informativa o correo electrónico
2	Mesa de Servicio	Recibe solicitud y levantara ticket para continuar con el proceso.	Ticket
3	Mesa de Servicio	Enviara correo a la persona superior jerárquica de la persona usuaria para solicitar la aprobación del servicio. ¿Se autoriza? Si, ir al paso 4 No, ir al paso 6	Correo electrónico
4	Mesa de Servicio	Asignará la solicitud al grupo de soporte para su atención.	
5	Grupo de Soporte	Informa a la Mesa de Servicio la atención a la solicitud.	
6	Mesa de Servicio	Informa la persona usuaria final sobre la atención de su requerimiento.	Correo electrónico
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



VIII.6 PROCEDIMIENTO PARA LA SOLICITUD DE ACCESO VÍA REMOTA VPN

OBJETIVO

Describir el orden de las acciones para que las personas usuarias tengan acceso a la red y/o recursos de infraestructura tecnológica, a través de cualquier equipo de cómputo o dispositivo vía remota VPN.

POLÍTICAS DE OPERACIÓN

1. Para solicitar algún servicio relacionado con los recursos de tecnologías de la información y/o comunicaciones remotas, se deberá enviar un oficio y/o correo electrónico a la Gerencia de Sistemas donde indique los motivos que sus actividades requieran mediante la entrega de la "RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)" (Anexo 1)

2. El personal de la Gerencia de Sistemas debe establecer por todos los medios, métodos, procesos, procedimientos y tecnologías disponibles y a su alcance, de las restricciones necesarias a los equipos y/o dispositivos que sean instalados y/o conectados a los recursos de la Red de Servicios de Diconsa, S.A. de C.V., así como la definición de roles, perfiles y permisos que sea estrictamente indispensables y mínimos para el cumplimiento de las labores encomendadas al personal.

3. Es responsabilidad de las personas usuarias el uso y aprovechamiento de Tecnologías de la Información, con privilegios de acceso local y/o remoto a la red corporativa, de asegurarse de que su conexión del acceso está sujeta a las restricciones definidas por la Gerencia de Sistemas para ese perfil específico.

4. El acceso remoto vía VPN es personal e intransferible.

5. La persona usuaria deberá resguardar de forma segura los elementos que le sean asignados para la instalación del servicio de VPN.

6. El acceso deberá realizarse desde un equipo de cómputo de la entidad, que cumpla con los requerimientos de la herramienta con la que se establecerá la conexión VPN.

7. Si la persona usuaria deja de laborar en el área donde se hizo la solicitud o por algún otro motivo deja de ser empleado activo, el superior jerárquico deberá de notificar a la Mesa de Servicio para la cancelación del servicio.

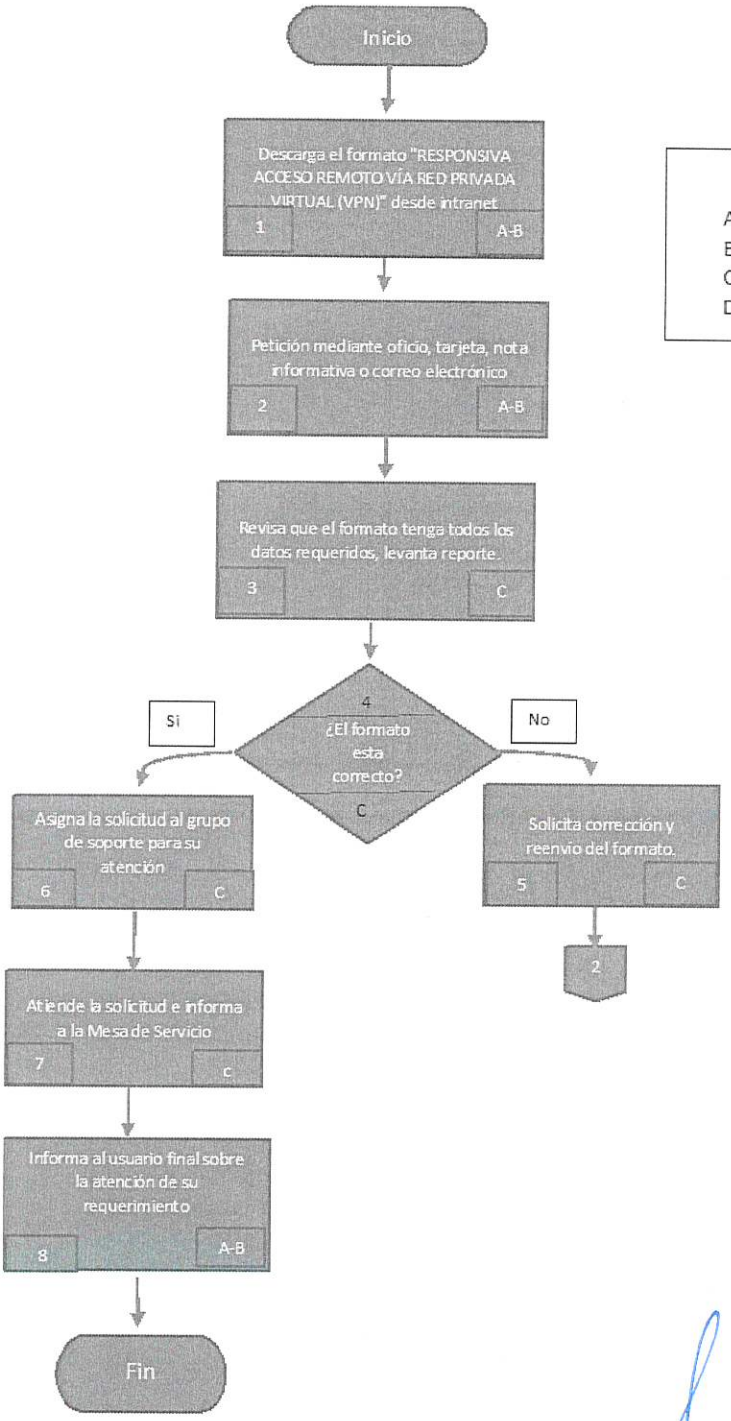
8. Si el servicio no presenta actividad en un periodo mayor a 90 días será dado de baja sin previo aviso.

9. Si el servicio es detectado en incumplimiento de las Políticas y/o Lineamientos de seguridad, será dado de baja de manera definitiva sin previo aviso.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	La persona Titular de área con ayuda de la persona Enlace Informático	Descargar el formato "RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)" desde la intranet.	RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)
2	La persona Titular de área con ayuda de la persona Enlace Informático	Petición por parte de la persona Titular de Área mediante Oficio, Tarjeta, Nota Informativa o correo electrónico enviando la responsiva firmada.	
3	Mesa de Servicio	Revisa que la responsiva presente todos los datos requeridos manteniendo comunicación la persona solicitante.	
4	Mesa de Servicio	Levanta ticket y asigna al grupo de soporte para su atención	Ticket
5	Grupo de Soporte	Atiende la solicitud e informa a la Mesa de Servicio.	
6	Mesa de Servicio	Se informa al usuario final sobre la atención de su requerimiento para el cierre del ticket.	Correo electrónico
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



RESPONSABLES

A. ENLACE INFORMÁTICO
B. TITULAR DE ÁREA
C. MESA DE SERVICIO
D. GRUPO SOPORTE

RELACIÓN DE ANEXOS

Número	Nombre del Documento	Clave
1	RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)	

ANEXO 1
RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)

SEGALMEX DICONSA | LICONSA S.A.	**Diconsa, Liconsa, Segalmex** **UNIDAD DE ADMINISTRACIÓN Y FINANZAS** GERENCIA DE SISTEMAS	HOJA	1 DE 2
		II.C	ASI
	ACTA RESPONSIVA ACCESO REMOTO VÍA RED PRIVADA VIRTUAL (VPN)	FECHA PUBLICACIÓN	01/03/2021
		FECHA ELABORACIÓN	01/03/2021
		ASI	

ASI- Administración de la seguridad de la información

Formato de asignación de usuario y contraseña para el servicio de acceso remoto por VPN

FOLIO No. **VPN-032**

Lugar y fecha:

Área: _____

Nombre: _____

Cargo: _____

Motivo de uso: _____

Como parte de la política de control de accesos y lineamientos específicos en materia de seguridad de la información que deben cumplirse, a fin de mantener la confidencialidad, integridad y disponibilidad de la información a la cual el personal tiene acceso como parte del desempeño de sus funciones, definidos en Acuerdo por el que se Modifican las políticas y disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información; la Gerencia de Sistemas hace entrega del siguiente nombre de usuario y contraseña para el acceso remoto VPN a la red de datos

Usuario:
Contraseña:

Asimismo, se hacen las siguientes recomendaciones para asegurar la confidencialidad del mismo:

a) Mantener la contraseña en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Notificar a la extensión **65162** cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

La guía de uso para la aplicación VPN será enviada por medio de correo electrónico con instalador y un manual de usuario de cómo debe de realizar la instalación.

En caso de encontrarse en una red con seguridad, los puertos que deberán ser permitidos en el firewall para que opere la conexión: Salida TCP ###, UDP ###, TCP ###

Para atención y asesoría, en la extensión 65120 y 65162.

Solicitante	Jefe Inmediato

Gerencia de Sistemas
Subgerente de Infraestructura y Telecomunicaciones SEGALMEX.

El incumplimiento de lo establecido en este documento será objeto de sanción administrativa en los términos de la Ley General de Responsabilidades Administrativas, independientemente de las sanciones de carácter penal que puedan desprenderse, conforme a la magnitud y característica del incumplimiento que se trate.

VIII.7 PROCEDIMIENTO PARA LA SOLICITUD DE RESPALDO DE INFORMACIÓN

OBJETIVO

Describir las actividades a seguir para que se realice el resguardo a medios magnéticos de la información generada de los diferentes documentos, inherentes a las actividades de la entidad, mediante el equipo de cómputo asignado para esta actividad.

POLÍTICAS DE OPERACIÓN

1. Es responsabilidad del área interesada o de la persona usuaria solicitar el respaldo de la información que estime necesaria.

2. El área interesada o la persona usuaria deberán proporcionar los medios de almacenamiento donde deba realizarse el respaldo, el cual deberá ser con algún medio con el que cuente la entidad.

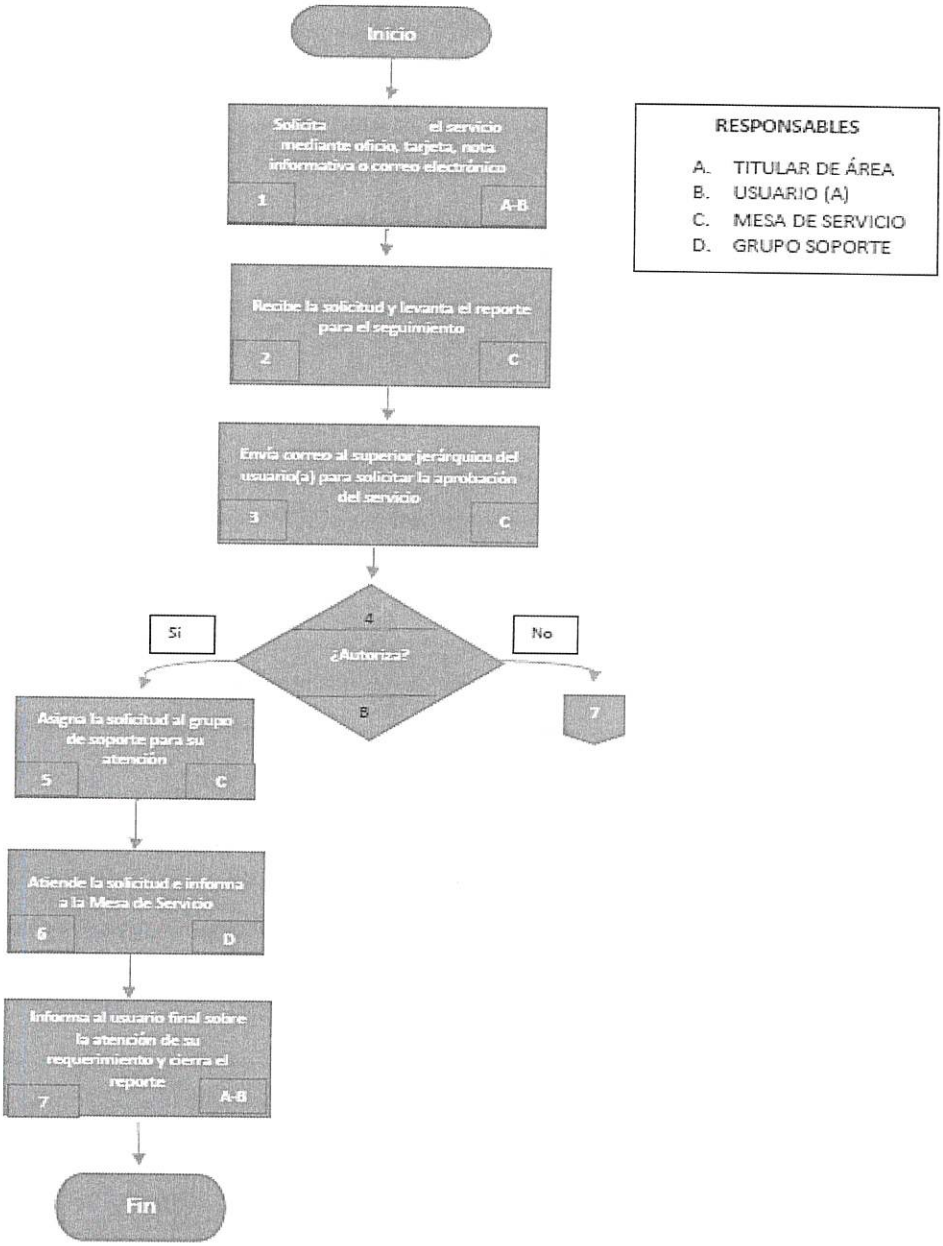
3. Solo procederá el respaldo de la información inherente al desarrollo de las actividades correspondientes a la entidad.

4. Será responsabilidad del área solicitante o de la persona usuaria el uso que se le dé a la información respaldada.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	La persona Titular de área o persona Usuaria	Solicita a la Gerencia de Sistemas realizar el respaldo de información requerido.	Oficio, Tarjeta, Nota Informativa o correo electrónico
2	Mesa de Servicio	Recibe solicitud y levantara ticket para el seguimiento.	Ticket
3	Mesa de Servicio	Asigna la solicitud al grupo de soporte para su atención	
4	Grupo de Soporte	Realiza el respaldo de la información en el medio magnético que le proporcione la persona usuaria e informa a la Mesa de Servicio la atención a la solicitud.	
5	Mesa de Servicio	Informa la persona usuaria final sobre la atención de su requerimiento.	Correo electrónico
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



VIII.8 PROCEDIMIENTO PARA EL MONITOREO DE USO DE INTERNET

OBJETIVO

Dar a conocer las acciones que la Gerencia de Sistemas realiza para identificar usuarios que hacen mal uso del servicio de Internet.

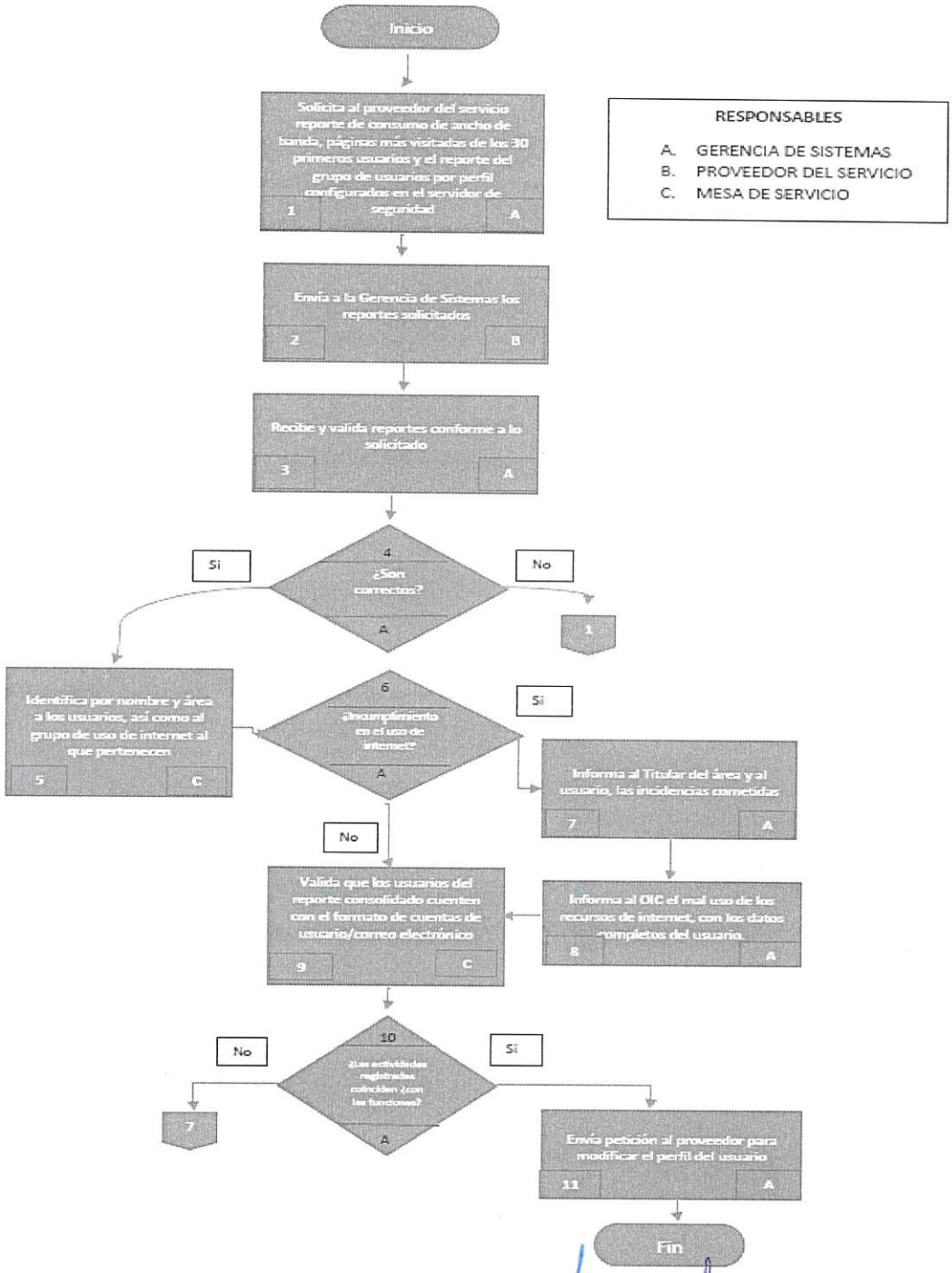
POLÍTICAS DE OPERACIÓN

1. Es responsabilidad de la Gerencia de Sistemas a través de la Subgerencia de Infraestructura y Telecomunicaciones monitorear el adecuado uso de Internet que hagan los usuarios de la entidad.
2. Se elaborará un reporte de consumo de ancho de banda y páginas más visitadas del servicio de Internet.
3. Es responsabilidad de los usuarios la utilización del servicio institucional de Internet, para asuntos relacionados con el desempeño de las funciones laborales o contractuales asociadas a sus funciones.
4. La Gerencia de Sistemas a través de la Subgerencia de Infraestructura y Telecomunicaciones identificara a las personas usuarias que incumplieron alguna política de uso de Internet.
5. La Gerencia de Sistemas a través de la Subgerencia de Infraestructura y Telecomunicaciones informará la persona Titular del área de la persona usuaria identificada y al implicado en estas conductas, las incidencias cometidas, asimismo se informará al área del Órgano Interno de Control, Autoridades Federales y Locales sobre el mal uso de los recursos del servicio de Internet con los datos completos de la persona usuaria involucrada.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Gerencia de Sistemas	Verificar el reporte que el proveedor envía en relación con el servicio de Internet, el consumo de ancho de banda y páginas más visitadas de los primeros 30 usuarios.	Correo electrónico.
2	Gerencia de Sistemas	Solicita al proveedor de servicio de Internet, reporte del grupo de usuarios por perfil configurados en el servidor de seguridad.	Correo electrónico.
3	Proveedor del Servicio	Envía a la Gerencia de Sistemas los reportes solicitados.	Correo electrónico.
4	Gerencia de Sistemas	Recibe y valida reportes conforme a lo solicitado. Si son correctos pasa a actividad 5. No son correctos, pasa a actividad 1.	Archivos en digitales
5	Gerencia de Sistemas	Identifica por nombre y área a las personas usuarias, así como al grupo de uso de internet al que pertenecen.	Ejecuta Instrucción de Trabajo 1.01. Reporte consolidado
6	Gerencia de Sistemas.	Identifica personas usuarias que incumplieron alguna política de uso de Internet. Si. Pasa a actividad 9. No. Pasa a actividad 7.	Reporte de incidencias
7	Mesa de Servicio	Valida que las personas usuarias identificadas en el reporte consolidado cuenten con el formato de cuentas de usuario/correo electrónico autorizado por su jefe inmediato superior de área.	Software de Gestión de Incidentes
8	Gerencia de Sistemas	Valida que las actividades registradas en el monitoreo coincidan con las actividades de sus funciones. Si, Pasa actividad 11. No, Pasa actividad 9.	Software de Gestión de Incidentes. / Reporte Excel.
9	Gerencia de Sistemas	Informa a la persona Titular del área y a la persona usuaria identificada las incidencias cometidas.	Correo electrónico
10	Gerencia de Sistemas	Informa al área del Órgano Interno de Control sobre el mal uso de los recursos del servicio de Internet con los datos completos de la persona usuaria involucrada.	Tarjeta Informativa
11	Gerencia de Sistemas	Envía petición a proveedor de servicio de Internet para modificar el perfil de usuario predeterminado o en su caso la cancelación del servicio.	Correo electrónico/Listado de grupos de uso de Internet.
		Fin del Procedimiento	

DIAGRAMA DE FLUJO



VIII.9 PROCEDIMIENTO PARA LA VALIDACIÓN DE CUENTAS DE USUARIO

OBJETIVO

Los privilegios en el acceso a los datos, servicios de información y de comunicaciones de todas las personas usuarias, deberán revisarse, con la finalidad de detectar comportamientos anormales o inactividad, a fin de garantizar que no se obtengan privilegios no autorizados.

POLÍTICAS DE OPERACIÓN

1. Es responsabilidad de la Gerencia de Sistemas la modificación e inhabilitación de cuentas de usuario del Directorio Activo y servidor de correo electrónico.
2. Las modificaciones necesarias a las cuentas de usuario serán realizadas por el administrador del servidor.
3. La Gerencia de Recursos Humanos deberá informar mensualmente los movimientos de personal que se lleven a cabo en la entidad.

DESCRIPCIÓN DE ACTIVIDADES

MENSUAL

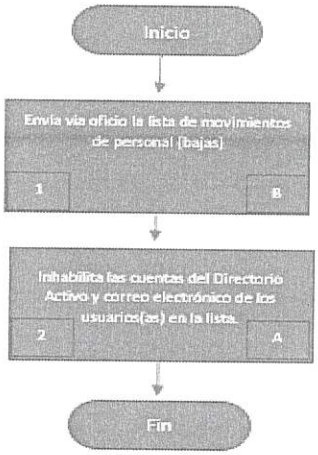
Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Gerencia de Recursos Humanos	Envía la lista de movimientos de personal (bajas) de forma mensual.	Reporte de Cuentas inhabilitadas
2	Gerencia de Sistemas	Inhabilita las cuentas de Directorio Activo y Correo de los usuarios en la lista.	
		Fin del Procedimiento	

TRIMESTRAL

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Gerencia de Sistemas	Genera un reporte de las Cuentas que están inhabilitadas por falta de uso (más de 30 días).	Reporte de Cuentas inhabilitadas
2	Gerencia de Sistemas	Compara el reporte de cuentas inactivas con los movimientos de Personal enviados por la Gerencia de Recursos Humanos.	
3	Gerencia de Sistemas	Notifica a la Gerencia de Recursos Humanos las cuentas inactivas para que valide si son personas usuarias vigentes.	Oficio
4	Gerencia de Recursos Humanos	Contesta la validación de las personas usuarias vigentes.	Oficio
5	Gerencia de Sistemas	Rehabilitan las cuentas de personas usuarias vigentes y se mandan las cuentas inactivas al grupo de cuentas deshabilitadas.	
6	Gerencia de Sistemas	Borra las cuentas deshabilitadas por más de 90 días.	
		Fin del Procedimiento	

DIAGRAMA DE FLUJO

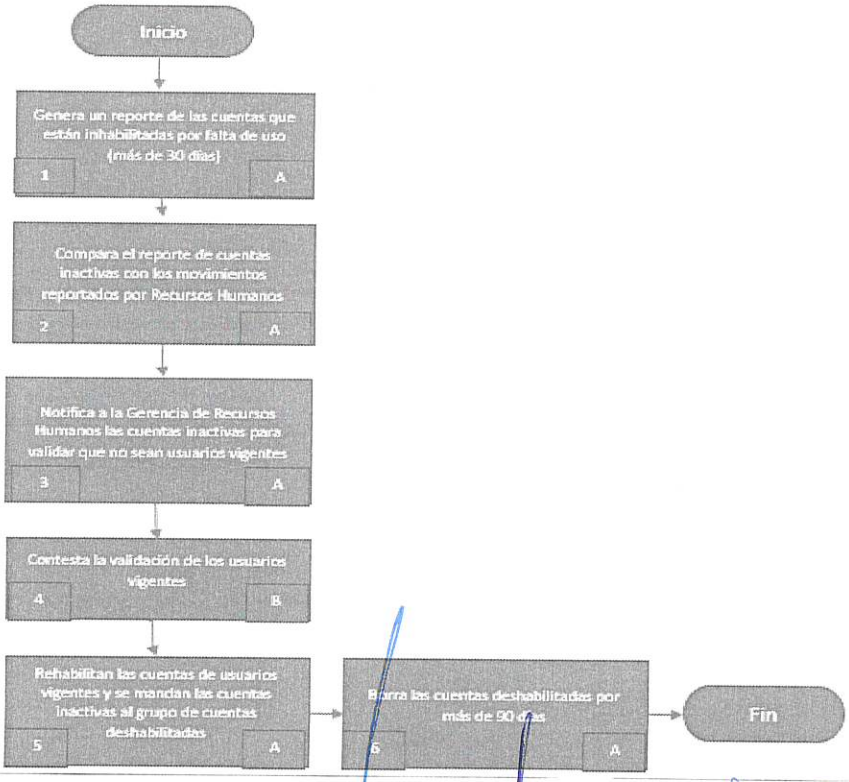
MENSUAL



RESPONSABLES

A. GERENCIA DE SISTEMAS
B. GERENCIA DE RECURSOS HUMANOS

TRIMESTRAL



VIII.10 PROCEDIMIENTO EN CASO DE ROBO, DAÑO O SINIESTRO

OBJETIVO

Describir el procedimiento y acciones necesarias a realizar para que las personas usuarias y/o responsables de equipos de cómputo, reporten el robo de su equipo de cómputo y/o accesorios.

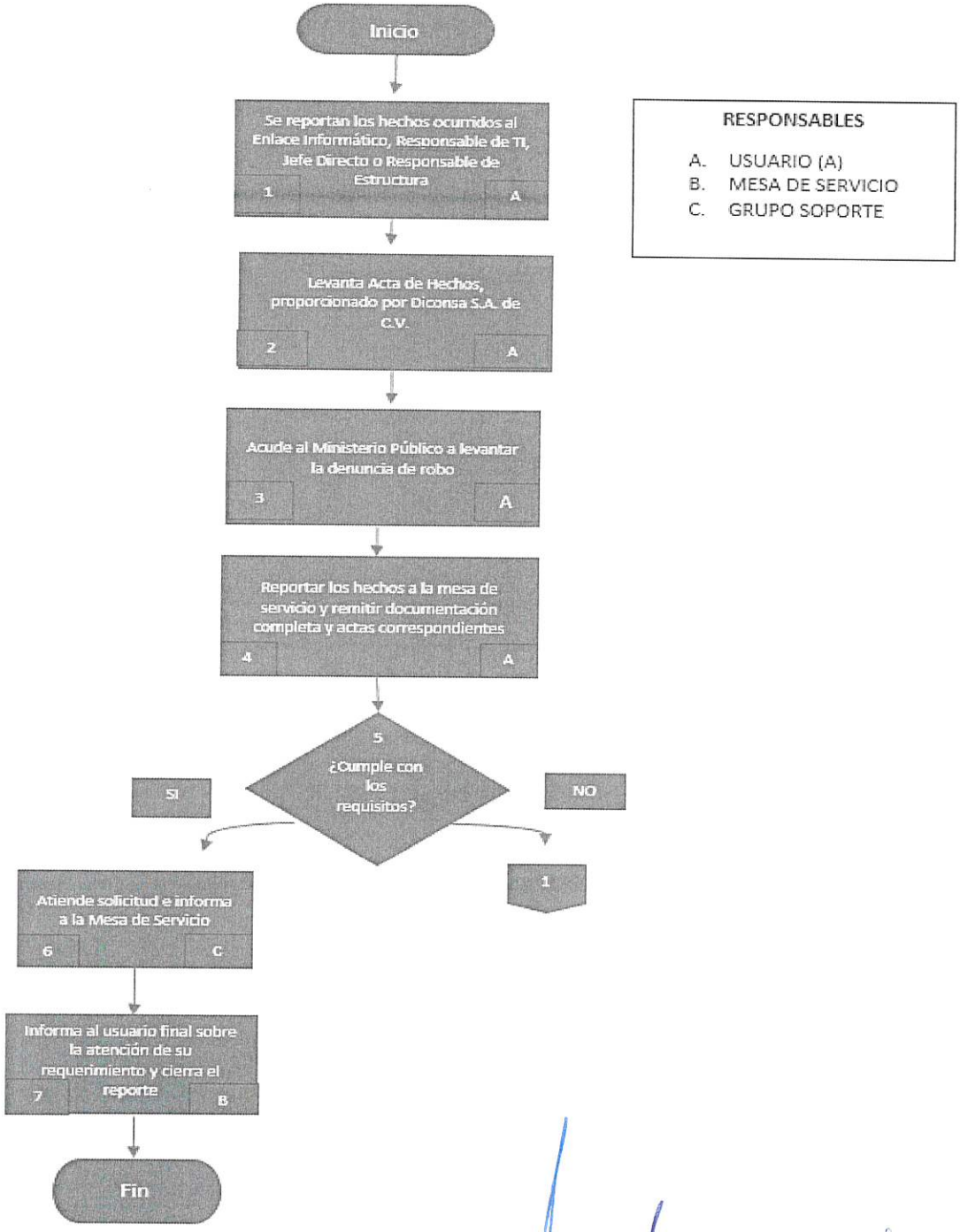
POLÍTICAS DE OPERACIÓN

1. La persona usuaria es responsable de informar a la Gerencia de Sistemas, sobre el robo, daño o siniestro del equipo de cómputo, tal y como lo establece la carta responsiva.
2. Es responsabilidad de la Gerencia de Sistemas levantar el ticket sobre la incidencia.
3. La persona usuaria es responsable de realizar las acciones pertinentes para reportar el robo del equipo de cómputo y/o accesorios.
4. La Gerencia de Sistemas deberá reportar al proveedor sobre el incidente.

DESCRIPCIÓN DE ACTIVIDADES

Paso Núm.	Responsable	Actividad	Nombre y clave del Documento de Trabajo
1	Usuario	Reporta los hechos ocurridos a su jefe directo	
2	Usuario	Levanta Acta de Hechos y/o denuncia de robo ante autoridades competentes	Acta de Hechos y/o Denuncia ante el Ministerio Público
3	Usuario	Acude al Ministerio Público a levantar la denuncia de robo	
4	Usuario	Reportar Hechos a la mesa de servicio y remite documentación completa, para generar su ticket y levantar el reporte correspondiente	Nota Informativa, Oficio o Correo Electrónico
5	Mesa de Servicio	Cumple con los requisitos Si, Pasa actividad 6 No, Pasa actividad 1	
6	Grupo de Soporte	Atiende Solicitud e informa a la Mesa de servicio	
7	Mesa de Servicio	Informa al usuario final sobre la atención de su requerimiento y cierra el reporte	
		Fin del procedimiento	

DIAGRAMA DE FLUJO



RELACIÓN DE ANEXOS

Número	Nombre del Documento	Clave
1	CARTA RESPONSIVA RESGUARDO DEL EQUIPO DE CÓMPUTO	

ANEXO 1
CARTA RESPONSIVA

CARTA RESPONSIVA

Ciudad de México, a ___ de _____ de 202_

Por medio de la presente, recibo de esta dependencia, el equipo de cómputo, marca _____, modelo _____, número de serie _____, como parte de las actividades que involucran mi cargo en esta dependencia, sobre el cual mantendré la custodia hasta el día que la dependencia lo requiera.

Comprendo que durante el período en el cual tenga el equipo de cómputo anteriormente descrito a mi cargo, en el área administrativa en la cual presto mis servicios, tengo la obligación de hacer buen uso del mismo, a fin de que el desempeño de mis funciones sea el óptimo para cumplir con los objetivos de esta dependencia, conservar el bien señalado en el presente documento y comprendo que no poseo autorización por parte de esta dependencia, ni de ningún representante, para utilizar el equipo de cómputo para fines personales, así como para poderlo prestar a ninguna persona que me lo requiera.

En caso de robo, daño o siniestro en el equipo de cómputo, me comprometo a denunciar el acontecimiento de forma inmediata ante esta dependencia y las autoridades correspondientes, a fin de que se realicen los procedimientos legales y administrativos correspondientes.

Asumo la responsabilidad sobre el mal uso del equipo de cómputo, así como de realizar las gestiones pertinentes a la brevedad y en caso de demora en la denuncia de tales acontecimientos a esta dependencia y a las autoridades correspondientes. En ese sentido autorizo a esta dependencia, a descontar de mi recibo de nómina o finiquito, en caso de terminar la relación laboral, el valor del equipo de cómputo o deducible. De igual manera acepto la responsabilidad del contenido de los archivos que se encuentren en el equipo de cómputo.

Declaro estar de acuerdo con lo anteriormente expuesto, y acepto la responsabilidad que me confiere en este momento al entregarme el equipo de cómputo materia de la presente carta responsiva.

ATENTAMENTE

_____
NOMBRE Y FIRMA DEL USUARIO

IX. HISTORIAL DE CAMBIOS

Revisión Núm.	Fecha de Autorización	Descripción del cambio	Motivo (s)
00	10-11-2022	Documento Nuevo	Creación de un manual cuyo objetivo es proporcionar a los usuarios de Diconsa, S.A. de C.V. una guía de buenas prácticas para el uso responsable de los Servicios de Tecnologías de la Información.

X. AUTORIZACIÓN DEL COMITÉ DE MEJORA REGULATORIA INTERNA

NOMBRE	FECHA	FIRMA
MTRO. ÁNGEL PEDRAZA LÓPEZ. Presidente del COMERI.		
LIC. HIRAM BENJAMÍN RUBIO GUZMÁN. Titular de la Unidad de Administración y Finanzas.		
LIC. FERNANDO DAVID PALOS IBARRA. Director Comercial.		
LIC. JESÚS SALVADOR VALENCIA GUZMÁN. Director de Operaciones de Diconsa.		
MTRO. DEMETRIO RODRÍGUEZ ARMAS. Director de Asuntos Jurídicos.		
ING. ROCÍO CORAZÓN GARCÍA SALAS. Titular del Órgano Interno de Control de SEGALMEX.		