PERIÓDICO OFICIAL

DEL GOBIERNO CONSTITUCIONAL DEL ESTADO DE MICHOACÁN DE OCAMPO

Fundado en 1867

Las leyes y demás disposiciones son de observancia obligatoria por el solo hecho de publicarse en este periódico. Registrado como artículo de 2a. clase el 28 de noviembre de 1921.

Directora: Mtra. Jocelyne Sheccid Galinzoga Elvira

Juan José de Lejarza # 49, Col. Centro, C.P. 58000 **DÉCIMA SECCIÓN** **Tel. 443-312-32-28**

TOMO CLXXXVI	Morelia, Mich., Jueves 17 de Octubre de 2024	NÚM. 66

CONTENIDO

GOBIERNO DEL ESTADO DE MICHOACÁN DE OCAMPO

SECRETARÍA DE FINANZAS Y ADMINISTRACIÓN

DIRECCIÓN GENERAL DE GOBIERNO DIGITAL

POLÍTICAS GENERALES EN MATERIA DE CIBERSEGURIDAD PARA LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA ESTATAL

LUIS NAVARRO GARCÍA, Secretario de Finanzas y Administración, en el ejercicio de las atribuciones que el titular del Ejecutivo me confiere con base en lo establecido en los artículos 62, 66 y 132 de la Constitución Política del Estado Libre y Soberano de Michoacán de Ocampo; artículos 9°, 11, 12 fracción XI, 17 fracción II y 19 fracciones LXXII y LXXIV de la Ley Orgánica de la Administración Pública del Estado de Michoacán de Ocampo, así como los artículos 6°, 16 y 20 del Reglamento Interior de la Secretaría de Finanzas y Administración; y,

C O N S I D E R A N D O

Que el Artículo 19 fracción LXXIV de la Ley Orgánica de la Administración Pública del Estado de Michoacán de Ocampo, establece que a la Secretaría de Finanzas y Administración le corresponde, entre otras funciones, «Coordinar y administrar las funciones de recolección de datos, almacenamiento, procesamiento y distribución de la información para el gobierno en red, así como la interacción con otros sistemas de información mediante la asesoría a las dependencias y entidades para la realización o contratación de servicios de las tecnologías de la información y comunicaciones, para el debido uso del sistema de gobierno en la red y desarrollo del gobierno digital que favorezcan la eficiencia, innovación y mejora de la gestión administrativa». Asimismo, establece el derecho a la buena administración, sustentada en los principios de accesibilidad, asequibilidad, calidad, continuidad, generalidad, progresividad y regularidad y garantiza que se tramiten los asuntos con diligencia, equidad, imparcialidad y oportunidad; basando la actuación de los servidores públicos en los principios rectores de legalidad, honradez, lealtad, imparcialidad, eficiencia, institucionalidad, transversalidad, gobernanza, transparencia, rendición de cuentas, sustentabilidad e igualdad sustantiva.

Que en el Plan de Desarrollo Integral del Estado de Michoacán de Ocampo 2021-2027 (PLADIEM) publicado en el Periódico Oficial del Estado, el Lunes 8 de Agosto de 2022, 6ª Secc. en la página 66, se contempla que la Secretaría de Finanzas y Administración, *además de reorganizar las funciones de cumplimiento de su objeto para eficientar las tareas de ingreso y rectoría en el ejercicio del gasto, se le confirieron facultades para hacer*

*realidad el **gobierno digital** como elemento fundamental para incrementar la eficiencia administrativa*. Los criterios del Eje transversal Gobierno Digital, Honesto, Eficaz y Transparente, presentes en la concepción de los objetivos, estrategias y líneas de acción del PLADIEM son referente de las acciones, programas y proyectos que se han implementado por la Secretaría de Finanzas y Administración a través de la Dirección General de Gobierno Digital en los siguientes aspectos:

1. Dotando de herramientas digitales que permitan que los servidores públicos se desempeñen con honestidad, honradez, ética, eficacia y eficiencia.

2. Combatiendo prácticas de corrupción y el uso inadecuado de los recursos públicos.

3. Promoviendo la transparencia y la rendición de cuentas.

4. Contribuyendo a reducir las brechas de desigualdad en el acceso al uso de las TIC, con criterios de inclusión y accesibilidad.

5. Transitando hacia el uso de la firma electrónica certificada, la reducción de documentos físicos y la digitalización de trámites y servicios.

Que el artículo 9º de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo, señala el principio de certeza, mismo que otorga seguridad y certidumbre jurídica a los particulares, en virtud de que permite conocer si las acciones del Instituto y sujetos obligados son apegadas a derecho y garantiza que los procedimientos sean completamente verificables, fidedignos y confiables; así como adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Que la Ley de Gobierno Digital del Estado de Michoacán de Ocampo, en su artículo 5° consigna como «obligación para los órganos del Estado el desarrollar, mantener y actualizar la infraestructura de tecnologías de la información y comunicaciones que garantice la transferencia, almacenamiento, procesamiento de información, la comunicación entre dependencias de la administración pública, así como la provisión de trámites y servicios de calidad a las y los ciudadanos». Asimismo, se establece en el artículo 13 de la Ley que: «[…] cada órgano del Estado podrá desarrollar, informando al consejo (*sic*), su propia Agenda Digital correspondiente». En este sentido es que la Secretaría de Administración a través de la Dirección General de Gobierno Digital ha generado ese documento rector, en su versión inicial: Estrategia de Gobierno Digital para las Dependencias y Entidades de la Administración Pública del Estado de Michoacán (2023); y actual: Agenda de Gobierno Digital para las Dependencias y Entidades de la Administración Pública del Estado de Michoacán, 2024.

Que en el artículo 81, fracción II de los Lineamientos Generales para la implementación del Gobierno Digital, Uso y Aprovechamiento Estratégico de Tecnologías de la Información y Comunicaciones del Estado de Michoacán de Ocampo contemplan que la Dirección General de Gobierno Digital es la unidad administrativa responsable de emitir el conjunto de buenas prácticas y lineamientos que cada dependencia y entidad deberá implementar en materia de ciberseguridad.

Por lo antes expuesto, he tenido a bien expedir las siguientes:

POLÍTICAS GENERALES EN MATERIA DE CIBERSEGURIDAD PARA LAS DEPENDENCIAS Y ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA ESTATAL

CAPÍTULO I
GENERALIDADES

1. JUSTIFICACIÓN.

Entendiendo el uso de plataformas tecnológicas en las funciones de gobierno, como una de las acciones más eficientes para acelerar los procesos de simplificación administrativa, resulta primordial prever acciones tendientes a la protección de la confidencialidad de la información y evitar poner en riesgo a los sujetos obligados; ya que la información es un activo indispensable, para todos los entes públicos al formar parte de los procesos de operación apoyando la toma de decisiones, por lo que la seguridad en su conservación se convierte en una prioridad para la administración pública.

Las amenazas latentes que pueden afectar a la información se derivan de las vulnerabilidades en los mecanismos de protección de la infraestructura tecnológica, provocadas por ataques de terceros, posibles auto ataques o por la deficiente aplicación de controles efectivos, toda vez que los sistemas y el tratamiento de información requieren estar protegidos; por lo que se recomienda implementar las medidas de seguridad y recomendaciones previstas en el presente documento.

En consecuencia, promover una cultura de concientización y responsabilidad sobre la importancia de contar con políticas de seguridad cibernética para la protección de los activos de información e informáticos en las unidades responsables de la administración pública, es una prioridad estratégica pues se fomenta su correcto resguardo, se promueve la precisión de los datos y su integridad, se asegura la disponibilidad y acceso a la misma, se valida la identidad de los usuarios y sistemas con accesos restringidos y se homologan criterios legales y estándares

de la industria para el cumplimiento de la normatividad aplicable en la materia.

Estos principios se enfocan en proteger los sistemas, redes y datos de las organizaciones y personas contra ciberataques y amenazas digitales, como *hackers*, *malware* y *phishing*. Al abordar estos aspectos, se puede reducir el riesgo de pérdida de datos y daños económicos y contribuir a que se garantice la seguridad y confianza en la gestión de la información.

2. OBJETIVO.

Establecer un marco integral que regule de manera eficiente y segura la concesión, gestión, revocación de accesos a los sistemas y recursos de las dependencias y entidades del Estado, propiciando que se garantice la protección de la información confidencial y reservada, minimizando riesgos de seguridad, fomentando la agilidad en la provisión y eliminación de privilegios de acceso, de conformidad con las normativas vigentes, así como las buenas prácticas de seguridad de la información, que posibiliten la creación y el uso de contraseñas robustas, únicas y seguras que permitan salvaguardar sistemas, datos confidenciales contra accesos no autorizados. Estas contraseñas seguras actúan como una barrera efectiva contra ataques cibernéticos, protegiendo la integridad, confidencialidad y disponibilidad de la información.

Estas políticas se destinan tanto a los colaboradores internos como al personal externo y pasantes autorizados o de servicio social, cuya participación en las operaciones de cada ente público, como sujetos obligados de la Ley, requieren de un medio de comunicación confiable y seguro para el intercambio de información relacionada con sus responsabilidades institucionales, tomando en cuenta la disponibilidad, seguridad y eficiencia de la infraestructura de red para respaldar las operaciones críticas y mejorar la prestación de servicios públicos; buscando la continuidad de las comunicaciones y operaciones de la administración pública, implementando medidas sólidas de seguridad para proteger la integridad de los datos, optimizar el rendimiento de la red y así mejorar la eficiencia operativa, respaldar operaciones críticas y establecer un marco para la mejora continua, adaptándose a las cambiantes necesidades tecnológicas y gubernamentales.

3. PROPÓSITO.

Asegurar un control riguroso y transparente en la concesión y revocación de accesos a los sistemas y datos de las dependencias y entidades del Estado, para facilitar privilegios de acceso, promover la responsabilidad en la gestión de las credenciales, y asegurar el cumplimiento normativo. Al establecer directrices claras sobre la creación, uso y almacenamiento de contraseñas, esta norma contribuye a organizar y controlar el acceso a los sistemas y recursos de información de manera adecuada y segura, teniendo como resultado el fortalecimiento de la seguridad en sistemas y datos al promover la adopción de mejores prácticas, así como también la prevención de posibles infracciones de datos; para mantener un inventario de activos digitales y periódicamente actualizarlo de acuerdo con el tiempo propuesto por el enlace responsable de TIC o unidad análoga al interior de los entes públicos. Esto permitirá realizar de manera más eficiente y precisa la creación de una topología sobre la infraestructura de activos físicos, estableciendo las medidas para el resguardo, asignación y garantía de acceso apropiado de los componentes tecnológicos. Asimismo, esta información servirá de base para determinar la gestión adecuada de los equipos tecnológicos acorde a las necesidades de la dependencia o entidad, obteniendo el máximo beneficio de las capacidades funcionales y de presupuesto asignado.

Consecuentemente, resulta necesario establecer un marco normativo robusto y claro que regule la utilización del servicio de correo electrónico proporcionado por las dependencias y entidades. Este marco tiene como objetivo principal fomentar un entorno laboral seguro, eficiente y colaborativo, donde el correo electrónico se utilice como una herramienta efectiva para facilitar la comunicación interna y externa, así como para respaldar las actividades laborales diarias de los colaboradores, personal externo y pasantes autorizados. Al establecer directrices claras y prácticas recomendadas para el uso adecuado de esta herramienta, estas políticas pretenden salvaguardar la seguridad, confidencialidad e integridad de las comunicaciones electrónicas, así como promover la responsabilidad y la conducta ética en su uso.

Además, se pretende optimizar el flujo de información dentro de las dependencias y entidades, mejorar la productividad y garantizar el cumplimiento de los objetivos institucionales mediante el uso eficiente y efectivo del servicio de correo electrónico; en última instancia, el propósito de estas políticas es fortalecer la integridad institucional, mantener la confianza de los colaboradores y contactos externos, contribuir al éxito y la eficacia de las operaciones de cada ente público.

Referente a la Infraestructura de Red para la protección del entorno de los entes públicos de la administración pública estatal con el fin de proporcionar lineamientos claros y coherentes para el diseño, implementación y mantenimiento de una red eficiente, segura y disponible. El propósito fundamental es optimizar la conectividad, promover la interoperabilidad de sistemas, garantizar, en la medida de lo posible, la integridad de los datos, y fortalecer la resiliencia de la infraestructura para respaldar las operaciones gubernamentales; fomentando buenas prácticas de gestión, mejorar la eficiencia operativa, asegurar la continuidad de las comunicaciones críticas y cumplir con los más altos estándares de seguridad cibernética.

4. ÁMBITO DE APLICACIÓN.

Estas políticas son aplicables a todas las personas servidoras públicas, trabajadores de base, confianza y eventuales, proveedores y cualquier sujeto que tenga acceso a los sistemas y datos de las dependencias o entidades de la Administración Pública Estatal centralizada y paraestatal del Estado de Michoacán. Incluye el uso de cuentas institucionales, dispositivos y aplicaciones en el entorno laboral, como

computadoras, teléfonos móviles, servidores y cualquier otro dispositivo conectado a las redes gubernamentales. Las pautas y criterios establecidos en estas políticas se harán del conocimiento general de los servidores públicos, trabajadores y colaboradores, y se aplicarán de manera consistente en todas las unidades responsables y niveles jerárquicos. Esto incluye la implementación de políticas de contraseñas seguras y la gestión de correos electrónicos proporcionados.

Para tomar decisiones sobre los activos informáticos, se debe contar con un informe detallado del estado y uso de dispositivos de usuario final, dispositivos de red y servidores, ya sean de propiedad de los entes públicos o de uso regular.

Son aplicables a este acuerdo las disposiciones de la Ley de Responsabilidades Administrativas para el Estado de Michoacán de Ocampo, por lo que los sujetos obligados señalados en estas políticas deberán sujetarse a sus preceptos. Ello implica que cualquier caso que configure una falta de las contenidas en la citada Ley, se deberá registrar y reportar la incidencia a los órganos evaluadores competentes con el apoyo de sus respectivos enlaces de Tecnologías de la Información y Comunicación (TIC) o unidades análogas, asegurando así una gestión adecuada y oportuna de las irregularidades que pudieran surgir.

5. GLOSARIO DE TÉRMINOS.

Acceso Físico: Capacidad de una persona o un sistema para entrar o interactuar con un dispositivo, sistema o lugar físico. En el contexto de la seguridad informática, el acceso físico a una computadora o servidor implica la capacidad de tocar y manipular la máquina directamente, lo que podría permitir a una persona tener control sobre ella, incluso si las medidas de seguridad lógica están en su lugar.

Activo: Elemento intangible digital que forma parte del patrimonio institucional y por su naturaleza generan valor monetario. Este valor está relacionado con el provecho que la administración les da a estos bienes. Ejemplo de ellos son: sistemas, plataformas, aplicativos y similares.

Administración remota: Capacidad de supervisar, configurar y mantener sistemas, dispositivos o redes desde una ubicación distante.

Autenticación reforzada: Método avanzado de verificación de identidad que va más allá de la simple autenticación de usuario con nombre de usuario y contraseña.

Autenticación: Proceso de verificar la identidad de un usuario, sistema o entidad para garantizar que sea quien afirma ser.

Autenticación en dos pasos (2FA): Medida de seguridad adoptada por empresas, organizaciones y personas para proteger el acceso a activos, recursos o aplicaciones digitales.

Autorización: Proceso mediante el cual se otorgan o niegan derechos y privilegios específicos a un usuario, sistema o entidad después de que se ha autenticado con éxito.

Brecha: Falla o vulnerabilidad en la seguridad de un sistema, red o aplicación que permite a personas no autorizadas acceder a información confidencial o realizar acciones no permitidas. Esta vulnerabilidad puede ser explotada por ciberdelincuentes para acceder a datos sensibles, como números de tarjetas de crédito, contraseñas u otra información privada.

Cadena de Confianza (*CoT*)**:** Serie de medidas y procesos que se implementan para garantizar la seguridad y la integridad de los datos y sistemas en un entorno informático. Esta cadena establece una secuencia de confianza que va desde el inicio hasta el final de un proceso o transacción, asegurando que cada componente, paso o entidad involucrada sea verificada y autenticada de manera adecuada antes de permitir su participación o acceso a recursos sensibles.

Certificado de Clave Pública: Tipo de certificado digital utilizado en criptografía de clave pública para autenticar la identidad de una entidad en línea, como un sitio *web*, una organización o un individuo.

Certificados Digitales: Documentos electrónicos utilizados para autenticar la identidad de entidades en línea, como personas, servidores, sitios *web* o dispositivos.

Cifrado: Proceso de conversión de datos en un formato ilegible o no comprensible, a través de la aplicación de un algoritmo matemático o criptográfico.

Ciberseguridad: Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio, redes privadas y públicas de telecomunicación.

Conectividad: Capacidad de dispositivos, sistemas o redes para establecer comunicación entre sí, permitiendo la transferencia de datos y la interacción.

Conexión: Establecimiento de un vínculo o enlace entre dos dispositivos, sistemas o redes para permitir la transmisión de datos o la

comunicación.

Confiabilidad: Capacidad de un sistema o servicio para funcionar de manera consistente y predecible, sin experimentar fallos o interrupciones significativas.

Control de Acceso: Gestión y regulación de quién tiene permiso para acceder a determinados recursos, sistemas, datos o instalaciones dentro de una organización o entorno específico.

Controles de Seguridad: Medidas, procedimientos, políticas, herramientas o acciones implementadas para proteger la información, los sistemas y los activos de una organización contra posibles amenazas, riesgos o vulnerabilidades.

Controles lógicos: Medidas y procedimientos implementados a nivel de *software* y sistemas informáticos para proteger la información, salvaguardar los activos digitales y garantizar la integridad, confidencialidad y disponibilidad de los datos.

Credenciales de Acceso: Información utilizada para identificar y autenticar a un usuario, permitiéndole acceder a sistemas, aplicaciones, redes o servicios.

Datos sensibles: Información que, debido a su naturaleza, requiere un tratamiento especial y cuidadoso debido a su potencial para causar daño o perjuicio si cae en manos equivocadas.

Dependencias y entidades de la administración pública estatal: Las Secretarías que conforman la Administración Pública Centralizada, establecidas en el artículo 17 de la Ley Orgánica de la Administración Pública del Estado de Michoacán de Ocampo; y Entidades, los Organismos Públicos Descentralizados, Empresas de Participación Estatal Mayoritaria, Fideicomisos Públicos y los demás que se establezcan conforme a las leyes de la materia; determinadas en el artículo 37 de la citada Ley.

DGGD: La Dirección General de Gobierno Digital de la Secretaría de Finanzas y Administración.

Dirección *IP*: Identificador numérico único asignado a cada dispositivo conectado a una red. La dirección *IP* permite que los datos se envíen de un dispositivo a otro a través de la red, de manera similar a cómo el correo se envía a una dirección física específica.

Dispositivos: Herramienta que se crea con un propósito específico, usualmente para facilitar una tarea o cumplir una función determinada.

Eficiencia: Capacidad de hacer las cosas de manera rápida y sin desperdicio en una red informática.

Enlaces responsables de TIC o unidad análoga: Las personas servidoras públicas responsables de las áreas de tecnologías, informática o cómputo de las dependencias y entidades, para dar cumplimiento material de la Ley de Gobierno Digital y demás normativa en la materia, encargados de la atención y soporte a los sistemas tecnológicos, sea equipos y *software*, para su funcionamiento adecuado y eficiente, así como de la mejora en la continuidad, reacción y recuperación de los servicios de TIC.

Enrutamiento de origen: Método de gestión de tráfico en una red que permite a un dispositivo, como un *router*, determinar la mejor ruta para enviar datos basándose en la información sobre la ubicación de origen de esos datos.

Enrutamiento estático: Método de configuración de rutas en una red de computadoras donde los administradores definen manualmente las rutas que los paquetes de datos seguirán a través de la red.

Escalabilidad: Capacidad de una red para crecer y adaptarse fácilmente a un mayor número de dispositivos o usuarios sin perder rendimiento.

Estándares: Reglas o pautas acordadas que establecen cómo deben diseñarse, operar e interactuar los dispositivos y sistemas. Estos estándares son cruciales para garantizar la consistencia, calidad, interoperabilidad o seguridad en un campo específico, así como la compatibilidad entre diferentes productos y tecnologías desarrollados por diversos fabricantes.

Filtrado de paquetes: Unidades de información que se envían a través de la red. El filtrado de paquetes implica examinar estos paquetes y decidir si permitir o bloquear su paso, según reglas establecidas.

***Firewall* basado en *host*:** Sistema de seguridad instalado directamente en un dispositivo individual, como una computadora o un servidor, para controlar y filtrar el tráfico de red.

***Firewall*:** Componente de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de datos entre una red privada y otra red, como internet.

***Firmware*:** *Software* que se encuentra incorporado en dispositivos electrónicos, como dispositivos de *hardware*, sistemas integrados y

componentes electrónicos.

***Hardware*:** Componentes físicos y tangibles de una computadora o dispositivo electrónico, como la pantalla, el teclado, el procesador, la memoria, los dispositivos de almacenamiento, los cables y otros elementos que conforman la estructura física de la máquina.

***Host* dedicado:** Servidor de computadora exclusivo para una sola entidad, como una empresa o un individuo. Un host dedicado ofrece un entorno más controlado y personalizado para alojar aplicaciones, sitios web o cualquier otra carga de trabajo.

***ICMP*:** Protocolo de comunicación en redes informáticas utilizado para enviar mensajes y realizar funciones de diagnóstico y control. *ICMP* es comúnmente asociado con herramientas como el comando «*ping*», que verifica la conectividad entre dispositivos en una red.

Identificador de Conjunto de Servicios (SSID): Nombre único que identifica una red inalámbrica. Es como el nombre de una tienda en un centro comercial que distingue esa red inalámbrica en particular de otras.

Impacto potencial: Evaluación de las posibles consecuencias, efectos o resultados que podrían surgir como resultado de una acción, evento o situación.

Infraestructura de red: Conjunto de elementos físicos y lógicos que forman la base de una red de comunicación.

Integridad: Calidad de los datos o la información que garantiza que no ha sido alterada de manera no autorizada o accidental.

Interfaz de Red: Componente o sistema que permite la conexión y comunicación entre un dispositivo, como una computadora, y una red de computadoras. La interfaz de red puede ser tanto *hardware* como *software*, y su función principal es facilitar la transmisión de datos entre el dispositivo y otros elementos de la red.

Interrupciones: Eventos inesperados que interrumpen o perturban el funcionamiento normal de un sistema, servicio o dispositivo.

LAN: Conjunto de dispositivos electrónicos, como computadoras e impresoras, que están conectados entre sí dentro de un área limitada, como una casa, una oficina o un edificio.

Líneas de consola: Conexiones físicas o virtuales que permiten la comunicación directa entre un usuario y un dispositivo, generalmente a través de una interfaz de línea de comandos.

***Malware*:** Tipo de *software* diseñado con intención maliciosa para dañar, interferir, robar datos o realizar acciones no autorizadas en un sistema informático, dispositivo o red.

Monitoreo: Proceso continuo de supervisión, medición y evaluación de actividades, sistemas, o entornos para obtener información relevante sobre su estado, desempeño o cambios.

Naturaleza del Acceso: Se refiere a la característica o tipo de acceso que una persona o sistema tiene a ciertos recursos o información. Puede variar desde ser un acceso abierto y completo a ser restringido y limitado.

Normativas: Conjuntos de reglas, directrices o requisitos establecidos por autoridades, organismos gubernamentales, o industrias para regular y estandarizar prácticas específicas.

OOB: Término que se refiere a la comunicación o gestión de datos que ocurre fuera del canal principal o de la vía convencional. Es como tener una línea de comunicación secundaria que se utiliza para propósitos especiales, generalmente para tareas de control, monitoreo o gestión.

Paquetes de multidifusión: En el contexto de redes de computadoras, los paquetes de difusión son mensajes que se envían a todos los dispositivos conectados a una red, sin tener una destinación específica.

Parche: Actualización de *software* diseñada para corregir, mejorar o actualizar un programa o sistema operativo. Siendo una solución que se aplica a un *software* existente para corregir errores, agregar nuevas funciones o mejorar la seguridad.

Pasarela de seguridad: Componente de red diseñado para proteger y gestionar el tráfico entre redes diferentes, como la red interna de una organización y la internet. Funciona como una barrera de seguridad que filtra, inspecciona y controla el flujo de datos, permitiendo una comunicación segura y protegiendo la red interna contra posibles amenazas externas.

Patrones de tráfico: Comportamientos repetitivos y predecibles observados en la transferencia de datos a través de una red de computadoras. Estos patrones pueden incluir la frecuencia de la comunicación, los tipos de datos transmitidos y las rutas comunes que siguen los datos.

Privilegio: Nivel de acceso, poder o autorización que se otorga a un usuario, programa, dependencia o entidad dentro de un sistema informático u organización. Estos privilegios determinan qué acciones, recursos o áreas del sistema pueden ser utilizados o accedidos por un sujeto o un *software*.

Proceso estructurado: Conjunto organizado de pasos o actividades diseñadas para lograr un objetivo específico de manera eficiente y consistente.

Protocolo: Conjunto de reglas y acuerdos preestablecidos que permiten la comunicación entre dispositivos o sistemas. Es como un idioma compartido que asegura que los diferentes componentes tecnológicos puedan entenderse y trabajar juntos de manera efectiva.

Protocolo *bootstrap*: Conjunto de reglas y procedimientos que permiten que un dispositivo se configure automáticamente al conectarse a una red.

Protocolo de Control de Transmisión *(TCP)*: Protocolo de comunicación en redes informáticas que proporciona una conexión confiable y ordenada entre dos dispositivos. TCP garantiza que los datos se transmitan de manera segura y completa, verificando la entrega de cada paquete y reorganizándolos en el orden correcto.

Protocolo de Datagramas de Usuario *(UDP)*: Protocolo de comunicación en redes informáticas que permite la transmisión rápida de datos entre dispositivos sin establecer una conexión previa y sin garantía de entrega.

Protocolo de Transferencia de Archivos *(FTP)*: Conjunto de reglas que facilita la transferencia de archivos entre computadoras a través de una red. Es como un servicio de mensajería que te permite enviar y recibir archivos de una ubicación a otra, como si estuvieras copiando archivos de una carpeta a otra.

Protocolo de Transferencia de Hipertexto *(HTTP)*: Conjunto de reglas que permite la transferencia de información en la *World Wide Web*. Es como el sistema de mensajería de la *web*, donde el navegador y los servidores web intercambian datos.

Protocolo Simple de Administración de Red (*SNMP*): Permite monitorear el rendimiento de los dispositivos, recibir alertas sobre problemas, e incluso realizar ajustes de configuración. Es como tener un sistema de comunicación estandarizado que permite a los dispositivos de red comunicarse y ser controlados de manera eficiente.

Protocolos de descubrimiento: Conjunto de reglas y procedimientos que permiten que dispositivos en una red se encuentren y reconozcan mutuamente automáticamente.

Puerta de enlace: Dispositivo o sistema que actúa como un punto de entrada o salida entre dos redes diferentes, permitiendo la comunicación y la transferencia de datos entre ellas.

Puerto: Número de identificación asignado a un proceso específico o servicio en un dispositivo. Estos números permiten que múltiples servicios se ejecuten en un solo dispositivo sin conflictos, ya que cada servicio utiliza un puerto único para la comunicación.

Puerto de origen: Número de identificación asociado al remitente de datos en una comunicación a través de una red. En términos sencillos, es como la «etiqueta de devolución» en un paquete enviado por correo: indica desde dónde se originó la información.

Punto de acceso: Dispositivo de red que permite la conexión inalámbrica de dispositivos a una red cableada existente mediante la tecnología *Wi-Fi*.

Punto de acceso inalámbrico: Dispositivo que permite la conexión de dispositivos electrónicos, como computadoras o teléfonos, a una red cableada e inalámbrica. Es como una «estación de conexión» que posibilita que tus dispositivos se conecten a internet o a una red local sin necesidad de cables.

Recursos tecnológicos: Herramientas, dispositivos y sistemas basados en tecnología que se utilizan para facilitar tareas, procesos y operaciones en diversos ámbitos.

Red: Conjunto de dispositivos electrónicos, como computadoras, impresoras o servidores, interconectados para compartir recursos y comunicarse entre sí.

Red conmutada: Infraestructura de comunicación en la cual se establecen conexiones temporales y exclusivas entre dos puntos para facilitar la transmisión de información.

Redundancia: Inclusión de elementos adicionales o duplicados en un sistema con el propósito de asegurar la continuidad del funcionamiento en caso de fallos.

Registro: Archivo o conjunto de datos que documenta eventos, actividades o transacciones específicas dentro de un sistema.

Rendimiento de la red: Eficiencia y calidad con la que los datos se transmiten y reciben a través de una red de computadoras.

Riesgo: Posibilidad de que ocurran eventos o situaciones que puedan tener impactos negativos en los objetivos, metas o activos de una organización o individuo.

***Router*:** Dispositivo de red que dirige el tráfico de datos entre redes o subredes, asegurando que los datos lleguen a su destino de la manera más eficiente posible.

Segmentación de Red: Práctica de dividir una red más extensa en segmentos más pequeños o subredes con el objetivo de mejorar la seguridad, el rendimiento y la administración.

Segmentos de Red: Cada segmento puede agrupar dispositivos que están físicamente cercanos, comparten ciertas funciones o tienen necesidades de seguridad similares. La segmentación facilita la administración y la implementación de políticas de red específicas para ese grupo particular de dispositivos.

Segregación: En el ámbito de la seguridad informática y de redes hace referencia a la práctica de separar o aislar ciertos componentes, sistemas o datos con el propósito de aumentar la seguridad, reducir riesgos y limitar el impacto de posibles amenazas.

Servidor: Computadora o un sistema informático que proporciona recursos, servicios, o funcionalidades a otras computadoras, conocidas como «clientes», dentro de una red.

Sistema de detección de intrusos: Herramienta de seguridad informática diseñada para monitorear y analizar la actividad en una red o sistema, identificando posibles intentos de violación de la seguridad.

Sistemas de respaldo de energía: Conjunto de dispositivos diseñados para proporcionar energía eléctrica adicional o continua en caso de interrupciones o fallas en el suministro principal.

***Software*:** Programas informáticos, conjunto de instrucciones y datos que permiten a una computadora realizar tareas específicas.

***Spam*:** Mensajes electrónicos no solicitados y generalmente no deseados que se envían en grandes cantidades, generalmente por correo electrónico, pero también a través de otros medios como mensajes de texto o redes sociales.

Subred: Porción lógica de una red *IP* más grande que ha sido subdividida para mejorar la administración y eficiencia en el enrutamiento de datos.

Telnet: Protocolo de red que permite a un usuario acceder y controlar remotamente otro dispositivo, como una computadora o un servidor, a través de la red.

Terminales virtuales: Permiten el acceso remoto a sistemas y la ejecución de comandos como si estuvieras físicamente presente en el lugar. Son útiles para administrar sistemas a distancia, facilitando la gestión y el control sin necesidad de estar físicamente en el mismo lugar que la máquina o servidor.

***Tokens*:** Contexto de la seguridad informática y la autenticación se refieren a un elemento o dispositivo utilizado para confirmar la identidad de un usuario durante un proceso de verificación.

Topología de Red: Estructura o patrón que describe cómo los dispositivos de una red de computadoras están interconectados. Puede verse como un mapa que muestra cómo los dispositivos, como computadoras, impresoras y enrutadores, están física o lógicamente conectados entre sí.

Topología: Estructura o patrón que describe cómo los dispositivos de una red de computadoras están interconectados. Puede verse como un mapa que muestra cómo los dispositivos, como computadoras, impresoras y enrutadores, están física o lógicamente conectados entre sí.

Tráfico de Red: Flujo de datos que viaja a través de una red de computadoras. Este flujo puede incluir la transferencia de archivos, correos electrónicos, solicitudes *web*, mensajes de *chat*, videoconferencias y cualquier otro tipo de comunicación digital entre dispositivos conectados en una red.

Tráfico no autorizado: Actividad de datos que ingresa o sale de una red sin la debida autorización o permiso. Este tipo de tráfico puede representar una amenaza para la seguridad de la red, ya que puede incluir actividades maliciosas, intentos de acceso no autorizado, o

violaciones a las políticas de seguridad establecidas.

Usuario final: Persona que utiliza un producto o servicio, especialmente en tecnología o software, para realizar tareas diarias, sin necesidad de conocimientos técnicos avanzados, responsable de informar al enlace responsable de TIC o unidad análoga, sobre cualquier cambio en su asignación o el estado de los activos de *hardware* que tiene asignados, así como utilizarlos de manera responsable y conforme a las políticas establecidas, incluyendo la protección física contra daños o pérdida.

Vida útil: Período de tiempo durante el cual se espera que dicho dispositivo funcione de manera adecuada y eficiente para cumplir con su propósito original. Esta medida se basa en diversos factores, incluyendo la calidad de los componentes, el diseño del dispositivo, el nivel de uso y mantenimiento, así como los avances tecnológicos que puedan volver obsoletos o menos funcionales ciertos dispositivos con el tiempo.

***Virtual Routing Forwarding* (*VRF*):** Técnica avanzada en el ámbito de las redes de computadoras que permite crear múltiples instancias virtuales de un enrutador dentro de un único dispositivo físico.

***VLAN*:** Tecnología de redes que permite segmentar una red física en múltiples redes lógicas, aislando grupos de dispositivos de manera virtual, aunque estén conectados a los mismos switches físicos.

***VPN*:** Tecnología que crea una conexión segura y cifrada entre un dispositivo y una red privada a través de internet, permitiendo al usuario enviar y recibir datos de manera segura a pesar de estar utilizando una red pública como internet.

Vulnerabilidades: Debilidades o fallos en sistemas, redes, aplicaciones o procesos que podrían ser explotados por amenazas externas para realizar acciones no autorizadas, comprometer la integridad de la información, o causar daños a un sistema o a una organización.

***WiFi Protected Access* 2 (*WPA*2):** Estándar de seguridad para redes *Wi-Fi* que proporciona una capa de protección para las comunicaciones inalámbricas.

***WiFi Protected Access* 3 (*WPA*3):** Estándar de seguridad para redes *Wi-Fi* que proporciona una capa adicional de protección para las comunicaciones inalámbricas. *WPA*3 reemplaza a su predecesor, *WPA*2, y mejora la seguridad al hacer más difícil que los atacantes descifren las contraseñas y accedan a la red.

Zona desmilitarizada: Área de una red que se encuentra entre una red interna segura y una red externa no confiable, como internet.

6. REVISIÓN Y EVALUACIÓN.

6.1. Las dependencias y entidades de la Administración Pública se deberán comprometer a realizar una revisión y evaluación continua de sus políticas, procedimientos y controles de seguridad, bajo la guía de DGGD, para garantizar la protección efectiva de sus activos de información. Este proceso se llevará a cabo de acuerdo con las siguientes directrices:

A) **Auditorías Internas:** Se realizarán auditorías internas de seguridad de manera periódica, con el objetivo de evaluar el cumplimiento de las políticas de seguridad establecidas y la efectividad de los controles implementados. Estas auditorías serán llevadas a cabo por el equipo de seguridad designado y se centrarán en áreas específicas de riesgo identificadas previamente;

B) **Análisis de Incidentes:** Se llevará a cabo un análisis detallado de los incidentes de seguridad reportados para identificar las causas subyacentes y las lecciones aprendidas. Esta información se utilizará para mejorar los controles de seguridad existentes y prevenir la recurrencia de incidentes similares en el futuro;

C) **Recopilación de Datos y Métricas:** Se recopilarán datos relevantes sobre incidentes de seguridad, tendencias de amenazas y métricas de cumplimiento para evaluar la efectividad de las medidas de seguridad implementadas. Estos datos se analizarán de manera regular para identificar áreas de mejora y tomar decisiones informadas sobre ajustes en las políticas y procedimientos de seguridad; y,

D) **Retroalimentación de los Usuarios Finales:** Se solicitará retroalimentación periódica de los usuarios finales y otras partes interesadas sobre la eficacia y la experiencia de usuario de las medidas de seguridad implementadas. Esta retroalimentación se utilizará para optimizar los controles de seguridad y garantizar que no afecten negativamente la productividad o la experiencia del usuario.

6.2. Los titulares de las dependencias y entidades, con sus respectivos enlaces de TIC o unidades análogas, serán responsables de que se ejecuten al interior de cada una las presentes políticas, con la asesoría de la DGGD.

6.3. Las dudas o controversias en la implementación de estas políticas, así como en su interpretación, que surjan en las dependencias

y entidades, serán resueltas por la DGGD, a través del Departamento de Ciberseguridad.

CAPÍTULO II
POLÍTICAS GENERALES DE CIBERSEGURIDAD

7. POLÍTICA DE LOS PROCEDIMIENTOS DE CONCESIÓN Y REVOCACIÓN DE ACCESO.

7.1. Concesión de acceso.

7.1.1. Todo acceso a sistemas y recursos de la dependencia o entidad por parte de las personas servidoras públicas deberá ser solicitado a través de un oficio dirigido a la persona responsable de TIC o con la unidad responsable. Esta solicitud deberá incluir la justificación del acceso solicitado, la aprobación de los directivos o departamento correspondiente, y cualquier otro detalle requerido.

7.1.2. La dependencia o entidad responsable deberá evaluar cada solicitud para determinar la legitimidad, la necesidad y los privilegios de acceso solicitados. Se verificará la autorización y se realizarán controles de seguridad para cerciorarse que la concesión de acceso cumpla con los requisitos y políticas establecidas.

7.1.3. Una vez aprobada, la concesión de acceso se deberá llevar a cabo de acuerdo con los privilegios definidos en la solicitud y aprobados por la autoridad correspondiente. Se proporcionarán credenciales y se informará al solicitante sobre las condiciones y responsabilidades asociadas con el acceso otorgado.

7.1.4. La concesión de accesos se basará en los principios de necesidad y mínimos privilegios, asegurando que cada persona servidora pública tenga acceso únicamente a la información y recursos necesarios para desempeñar sus responsabilidades laborales de manera efectiva.

7.1.5. Se deberán realizar cambio de contraseñas a correos electrónicos de manera periódica, en un término no mayor a dos meses.

7.2. Criterios de Concesión de Acceso.

7.2.1. Todo usuario que solicite acceso a los sistemas y recursos de la dependencia o entidad debe ser identificado de manera única. Se deberá requerir primordialmente el uso de credenciales individuales, como nombres de usuario y contraseñas, tokens de autenticación de dos factores, certificados digitales u otros medios aprobados para verificar la identidad.

7.2.2. Se deberán mantener las credenciales de acceso de forma segura. Se recomienda cambiar las contraseñas periódicamente y no compartirlas con terceros, además de seguir las directrices de complejidad establecidas, tomando como base el apartado correspondiente de las presentes políticas.

7.2.3. Se deberá implementar la segregación de deberes para limitar los privilegios de acceso y reducir el riesgo de conflictos de intereses o posibles adulteraciones en los datos. Los roles y responsabilidades se definirán claramente, evitando la acumulación excesiva de privilegios.

7.3. Roles y permisos.

7.3.1. Se deberán establecer roles predefinidos que reflejen las responsabilidades laborales dentro de las dependencias y entidades. Estos roles estarán asociados a conjuntos específicos de tareas y privilegios de acceso.

7.3.2. Cada rol deberá tener una descripción detallada que especifique las funciones, responsabilidades y los permisos asociados a dicho rol. Esto garantizará una comprensión clara de las expectativas y los límites de cada rol.

7.3.3. Se deberá llevar a cabo una revisión periódica de los roles asignados para garantizar que sigan siendo apropiados y se ajusten a las tareas realizadas por los usuarios.

7.3.4. Cada rol deberá tener asociado un conjunto de permisos que determinarán el acceso a los sistemas, aplicaciones y datos. Estos permisos deberán estar claramente definidos y documentados.

7.4. Acceso a Datos Sensibles.

7.4.1. Se debe establecer un proceso de clasificación de datos para identificar y etiquetar la información sensible. Esto incluirá información confidencial, personal, financiera o cualquier otro tipo de datos considerados sensibles en uso en la Dependencia o entidad como lo refiere la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de

Michoacán de Ocampo y la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo.

7.4.2. Se deberá mantener un inventario actualizado que detallará la ubicación, el tipo de datos y las personas con acceso a esta información sensible.

7.4.3. El acceso a datos sensibles estará restringido únicamente a usuarios autorizados que necesiten dicha información para el desempeño de sus atribuciones y funciones laborales.

7.4.4. Los responsables de TIC o unidades análogas de los entes públicos deberán implementar medidas de seguridad específicas para la protección de datos sensibles, como el cifrado, la monitorización de accesos, controles de acceso basados en roles, entre otras prácticas recomendadas.

7.4.5. Se deben establecer controles estrictos para el acceso a datos sensibles, incluyendo autenticación reforzada, limitación de acceso basada en necesidad, y revisión continua de privilegios.

7.5. Periodos de Validez de Acceso.

7.5.1. Todo acceso otorgado deberá tener un período de validez inicial claramente definido. Este período se establecerá en función de la naturaleza del acceso y las necesidades operativas del colaborador, estas acciones estarán sujetas a revisión y renovación periódica.

7.5.2. Se deberá implementar un proceso formal y documentado para la renovación del acceso una vez que el período inicial esté por expirar. Esto puede incluir la verificación de la necesidad continua del acceso y la actualización de credenciales de acuerdo con las políticas establecidas.

7.5.3. Se deberán llevar a cabo revisiones periódicas para evaluar la necesidad continua del acceso y asegurarse de que siga siendo relevante para las responsabilidades laborales del usuario.

7.6. Revocación de acceso.

7.6.1. Todos los accesos, donde las personas servidoras públicas, trabajadores de base, confianza y eventuales, proveedores o cualquier sujeto que con causa justificada tenga acceso a los sistemas y datos que puedan ocasionar intencionalmente, perjuicios materiales durante el desempeño de las labores o con motivo de ellas, en los edificios, obras, maquinaria, instrumentos, materias primas y demás objetos relacionados con el trabajo tanto físicos como lógicos, en los activos asignados para el cumplimiento de sus responsabilidades y ejercicio de sus atribuciones y funciones podrán ser revocados. Estos activos incluyen, pero no se limitan a los siguientes:

a) Cuentas institucionales de correo electrónico;

b) Documentos tanto en formato físico o digital, que contengan información referente al ejercicio de las funciones del miembro del personal;

c) Acceso físico a cualquiera de los edificios u oficinas de trabajo de la entidad;

d) Acceso físico y lógico a cualquiera de las redes *LAN, MAN y VPN* de la dependencia o entidad; y,

e) Credenciales de acceso a dispositivos tales como: impresoras, computadoras, correos electrónicos institucionales, servidores, entre otros.

7.6.2. En el caso de necesitar revocar el acceso, se seguirá un procedimiento definido y documentado. Esta acción será llevada a cabo por la persona servidora pública responsable de TIC o titular de la unidad administrativa autorizada para dicho fin, en conformidad con los procedimientos de seguridad y control establecidos dentro de la dependencia o entidad.

7.6.3. Se notificará al usuario afectado sobre la revocación de sus privilegios de acceso. Además, se mantendrá un registro detallado de las acciones de revocación, incluyendo la justificación, la fecha y la identidad de la persona que realizó la revocación.

8. POLÍTICA DE LA CREACIÓN, USO Y ENTREGA DE CONTRASEÑAS.

8.1. Se deberá establecer cierta complejidad en el uso y establecimiento de contraseñas teniendo en cuenta los siguientes puntos:

a) Las contraseñas deben tener una longitud mínima de 12 caracteres y contener una combinación de letras mayúsculas y minúsculas, números y símbolos; y,

b) Evitar el uso de información personal fácilmente identificable, como nombres propios, fechas de nacimiento o palabras comunes.

8.2. Se debe establecer un periodo específico para el cambio de contraseñas con un lapso mínimo de 30 días y un máximo de 90. De igual forma, no se deberá hacer uso de contraseñas antiguas y deberán ser únicas para cada una de las cuentas y sistemas asignadas a un usuario.

8.3. Se deberá establecer el uso de autenticación multifactorial, de tal manera que exista una capa extra de seguridad al momento de realizar accesos de cualquier tipo.

8.4. Debe prohibirse el almacenamiento de contraseñas en documentos no seguros, tales como hojas de cálculo, notas o correos electrónicos sin cifrar.

8.5. Las contraseñas pertenecientes a cada usuario deberán ser únicas e intransferibles, por lo que no deberán ser compartidas a ningún otro usuario en circunstancias normales.

8.6. Se deberán establecer procedimientos para monitorear el uso de contraseñas y detectar actividades sospechosas o intentos de acceso no autorizados.

8.7. En caso de sospecha o vulneración de alguna cuenta o sistema por compromiso de contraseñas, el incidente deberá ser reportado a la brevedad posible a la DGGD, para que esta la canalice dependiendo de la naturaleza que trate, al área que la atenderá.

8.8. Se deberán implementar mecanismos de bloqueo de cuentas después de un número determinado de intentos fallidos de inicio de sesión, y establecer procesos seguros de recuperación de contraseñas.

8.9. Se deberá realizar evaluaciones periódicas de riesgos para determinar la efectividad de los requisitos actuales de contraseña y ajustarlos según sea necesario para abordar nuevas amenazas.

8.10. Del procedimiento de entrega de usuarios, contraseñas y correos electrónicos institucionales para los Servidores Públicos de dependencias y entidades:

8.10.1. Solicitud: La DGGD será la unidad que otorgue los controles de acceso a los sistemas, plataformas, aplicaciones y de más recursos del entorno digital del Estado con los que cuente y sea susceptible de entregar mediante previa solicitud del titular de la dependencia o entidad o titular de la unidad responsable, para asignar al servidor público de que se trate, el usuario, los roles y permisos necesarios para el desempeño de sus funciones, anexando copia del nombramiento con que se ostenta.

8.10.2. Asignación de usuario: La DGGD, a través de la Dirección de Infraestructura y Sistemas, entregará al servidor público en sobre cerrado el usuario, contraseña inicial y un correo electrónico institucional en caso de aún no tenerlo.

8.10.3. Control de Uso y las responsabilidades que implican: Cada usuario será responsable del mecanismo de control de acceso que se le proporciona, esto es, de su clave de usuario y contraseña necesario para el acceso y uso de los recursos e información del Entorno Digital del Estado, por lo cual deberá mantenerlo en forma confidencial.

a) El acceso a la plataforma o sistema será para el ejercicio exclusivo de las atribuciones que le corresponden conforme al nivel de responsabilidad del usuario;

b) La clave de usuario autorizada es de uso personal, intransferible, inmutable e institucional, y será responsabilidad exclusiva del usuario el manejo que en dicha clave se ejecute, siendo susceptible a las sanciones aplicables, por lo tanto, no está permitido el uso de la misma clave de usuario por varios usuarios y está prohibido compartir la contraseña. Así mismo está prohibido divulgar, transferir, publicar, prestar o suplantar el acceso a la Plataforma o Sistema;

c) Al realizar el primer acceso con la clave asignada, el usuario deberá cambiar la contraseña inicial, asimismo, deberá realizar periódicamente su cambio. En caso de sospecha de que la contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente y notificar a su superior esta situación, así como la posible intrusión, para deslindar responsabilidad en caso necesario;

d) Cualquier cambio en los roles, perfiles y responsabilidades del usuario que modifique sus privilegios de acceso al

sistema o plataforma a que hace referencia en este documento, deberá ser notificado por escrito a la DGGD, por el titular del área respectiva, a fin de realizar el ajuste. La vigencia de la clave es indefinida, en tanto continue la relación laboral. Po lo que, en la misma forma, se deberá solicitar la baja y/o cancelación de la clave de usuario, de manera inmediata a la separación del servicio del usuario, por cualquier circunstancia; y,

e) Si el usuario olvida, bloquea o extravía su contraseña, deberá reportarlo por escrito a la DGGD, para que se le proporcione una nueva, podrá hacerlo por correo electrónico dirigido a **mesadeservicio@sfa.michoacan.gob.mx,** o por mensaje de *WhatsApp* al número **443 4823248**, donde el usuario podrá solicitar ayuda; soporte técnico o notificar lo conducente.

8.10.4. Conciencia de hacer un mal uso de los datos con responsabilidad civil, laboral, penal, fiscal y/o administrativa: De conformidad con los artículos 97 y 102 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo, por lo que usar, sustraer, divulgar, compartir con terceros sin su consentimiento, utilizarlos para fines distintos a los que fueron recabados, venderlos o rentarlos a terceros, conservarlos por más tiempo del necesario, no protegerlos adecuadamente, transferirlos, utilizarlos para discriminar o dañar su reputación, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, la información que se encuentre bajo su custodia como servidor público o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión conforme a las facultades correspondientes puede estar sujeto a sanciones conforme a lo previsto en el Capítulo II de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo (LTAIPPDPEMO)**,** así como del orden civil, penal, administrativa o penal que procedan conforme a lo previsto en los artículos 210, 211, 211 BIS, 211 bis 1, 211 bis 7, 214 fracción IV del Código Penal Federal y demás relativos y aplicables de la legislación federal.

8.10.5. Aceptación y compromiso: Las personas servidoras públicas que reciban la clave de usuario y contraseña inicial deberán firmar un documento que incluye:

a) Los datos del solicitante (cargo, dependencia o entidad y/o unidad responsable, número de oficio de la solicitud, fecha de asignación);

b) Los datos de la persona autorizada (a quien se asigna el usuario y el cargo o área de adscripción);

c) La asignación de usuario (sistema, aplicación o plataforma para la que se asigna, usuario asignado, contraseña inicial y el rol o perfil de acceso);

d) Un apartado sobre el control de uso del usuario;

e) Manifestaciones de confidencialidad y responsabilidad;

f) La aceptación del funcionario público, incluyendo su nombre, fecha y firma autógrafa; y,

g) La firma, cargo y correo electrónico institucional del representante de la DIS que entrega la clave de usuario asignada.

8.10.6. Contacto de quien entrega: Para cualquier duda o aclaración, el servidor público puede contactarse con la DIS a través del correo electrónico institucional proporcionado en el documento de aceptación.

8.11. Del procedimiento interno de entrega de usuarios, contraseñas y correos electrónicos institucionales para los servidores públicos:

8.11.1. Para el caso de correos electrónicos institucionales, se deberá solicitar el usuario, contraseña por oficio dirigido a la DGGD, y en los que se realicen entregas de contraseñas, accesos a plataformas, sistemas o páginas, que sean desarrollos propios, legados o adquiridos, internamente, la dependencia o entidad deberá realizarlo por escrito en sobre cerrado y considerando los siguiente:(sic).

8.11.2. Control de uso y las responsabilidades que implican: Cada usuario será responsable del mecanismo de control de acceso que se le proporciona, esto es, de su clave de usuario y contraseña necesario para el acceso y uso de los recursos e información del Entorno Digital del Estado, por lo cual deberá mantenerlo en forma confidencial:

a) El acceso a la plataforma o sistema será para el ejercicio exclusivo de las atribuciones que le corresponden conforme al nivel de responsabilidad del usuario;

b) La clave de usuario autorizada es de uso personal, intransferible, inmutable e institucional, y será responsabilidad

exclusiva del usuario el manejo que en dicha clave se ejecute, siendo susceptible a las sanciones aplicables, por lo tanto, no está permitido el uso de la misma clave de usuario por varios usuarios y está prohibido compartir la contraseña. Así mismo está prohibido divulgar, transferir, publicar, prestar o suplantar el acceso a la Plataforma o Sistema;

c) Al realizar el primer acceso con la clave asignada, el usuario deberá cambiar la contraseña inicial, asimismo, deberá realizar periódicamente su cambio. En caso de sospecha de que la contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente y notificar a su superior esta situación, así como la posible intrusión, para deslindar responsabilidad en caso necesario; y,

d) Cualquier cambio en los roles, perfiles y responsabilidades del usuario que modifique sus privilegios de acceso al sistema o plataforma a que hace referencia en este documento, deberá ser notificado por escrito al superior jerárquico directo y en su caso a la DGGD, a fin de realizar el ajuste. La vigencia de la clave prevalecerá en tanto continue la relación laboral. Por lo que, en caso de rescisión laboral o cambio de cargo, se deberá solicitar la baja o cancelación de la clave de usuario, de manera inmediata a la separación del servicio del usuario, por cualquier circunstancia.

8.11.3. Conciencia de hacer un mal uso de los datos con responsabilidad civil, laboral, penal, fiscal y/o administrativa: De conformidad con los artículos 97 y 102 de la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo, por lo que usar, sustraer, divulgar, compartir con terceros sin su consentimiento, utilizarlos para fines distintos a los que fueron recabados, venderlos o rentarlos a terceros, conservarlos por más tiempo del necesario, no protegerlos adecuadamente, transferirlos, utilizarlos para discriminar o dañar su reputación, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente, sin causa legítima, la información que se encuentre bajo su custodia como servidor público o a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión conforme a las facultades correspondientes puede estar sujeto a sanciones.

8.11.4. Aceptación y compromiso: El funcionario público que reciba la clave de usuario y contraseña inicial deberá firmar un documento que deberá incluir:

a) Los datos del solicitante (cargo, dependencia o entidad o unidad responsable, número de oficio de la solicitud, fecha de asignación);

b) Los datos de la persona autorizada (a quien se asigna el usuario y el cargo o área de adscripción);

c) La asignación de usuario (sistema, aplicación o plataforma para la que se asigna, usuario asignado, contraseña inicial y el rol o perfil de acceso);

d) Un apartado sobre el control de uso del usuario;

e) Manifestaciones de confidencialidad y responsabilidad;

f) La aceptación del funcionario público, incluyendo su nombre, fecha y firma autógrafa; y,

g) La firma, cargo y correo electrónico institucional del representante de la DIS que entrega la clave de usuario asignada.

9. POLÍTICA DE LA GESTIÓN DE INVENTARIO Y CONTROL DE ACTIVOS DE *HARDWARE*.

9.1. Gestión de inventario.

9.1.1. Los activos deben estar debidamente registrados en una bitácora para un mayor control y ubicación de los mismos, con la finalidad de evitar pérdidas o aprovechamiento de los recursos. La bitácora debe contener al menos los siguientes rubros:

a) Nombre del dispositivo;

b) Fecha de adquisición;

c) Estado;

d) Propietario del activo;

e) Departamento al cual pertenece;

f) No. de serie del dispositivo;

g) Sistema operativo;

h) Si tiene o no autorización para conectarse a la red;

i) Cada activo debe estar asociado a un identificador o etiqueta; y,

j) Especificaciones técnicas.

9.1.2. Los activos tecnológicos asignados a usuarios finales deberán ser respaldados por medio de la firma de un formato de carta en el cual se específique que el uso y asignación de activos será única y exclusivamente para el cumplimiento de actividades pertenecientes a la entidad.

9.1.3. Se deberá implementar algún *software* que permita la gestión del inventario actual de hardware. Tal *software* podrá ser con licencia o sin licencia, pero sí deberá gestionar y almacenar las características de cada dispositivo, de tal manera que la información sea útil cuando se requiera.

9.1.4. La topología de la infraestructura deberá estar documentada en su totalidad por el enlace responsable de TIC o unidad análoga, incluyendo todos los equipos con los que se cuente, sus características, área o departamento a los cuales están asignados, así como también un diagrama de red que permita identificarlos de manera lógica. Dicha topología deberá estar disponible para todo el personal de servicio apropiado.

9.1.5. Los enlaces responsables de TIC o unidades análogas de las dependencias y entidades definirán los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación y realizar la respectiva actualización del inventario con el que se cuenta de acuerdo con los procesos establecidos por la propia dirección. Considerando lo siguiente:

a) Equipo que se encuentre en su ciclo final de vida y no cuente con soporte de mantenimiento por parte de los fabricantes, deberá ser reemplazado por uno de nueva generación.

9.2. Control de activos de *hardware*.

9.2.1. Los enlaces responsables de TIC o unidades análogas de las dependencias y entidades serán los encargados de verificar si se requiere algún cambio y/o soporte para cualquier activo de la dependencia bajo el procedimiento definido por el mismo.

9.2.2. Para el proceso de adquisición de activos de *hardware*, se deberá adquirir equipo nuevo únicamente en caso de que no se encuentre en el inventario y este no esté en uso con la finalidad de contar con un aprovechamiento de los recursos y reducir costos.

9.2.3. De acuerdo al tipo de activo del cual se requiera hacer uso, podrá cambiar el personal autorizado y para ello se contempla lo siguiente:

a) Solo personal adscrito podrá hacer uso de las impresoras pertenecientes a las dependencias o entidades;

b) Los dispositivos móviles pertenecientes a personal base, de confianza o usuarios autorizados deberán respetar las políticas de uso dentro de las instalaciones; y,

c) El uso de dispositivos que no se encuentren a nombre de la dependencia o entidad deberán ser permitidos únicamente si se autoriza al usuario el utilizarlos. Dígase dispositivos como computadoras, *tablets*, discos duros o algún otro tipo de medio de almacenamiento.

9.2.4. Los activos de *hardware* únicamente podrán ser adquiridos por proveedores autorizados y registrados dentro del Padrón de Proveedores del Ejecutivo del Estado, en apego al artículo 5º de Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Prestación de Servicios Relacionados con Bienes Muebles e Inmuebles del Estado de Michoacán de Ocampo, para el Ejercicio Fiscal que corresponda y demás aplicables de la Ley de Adquisiciones, Arrendamientos y Prestación de Servicios relacionados con Bienes Muebles e Inmuebles del Estado de Michoacán de Ocampo, de conformidad con el monto a erogar, así como la Guía Técnica para Adquisición de Equipo de Cómputo.

9.2.5. Se deberá establecer una cadena de confianza (*CoT*) la cual se encargue de validar cada componente de *hardware*, mediante un certificado de clave pública que identifique la autoridad del mismo. De esta manera será posible llevar una mejor

administración con respecto a lo que está permitido (y lo que no) para dispositivos de usuario final.

10. POLÍTICA DE LA PROTECCIÓN Y USO DE CORREO ELECTRÓNICO.

10.1. Los usuarios son responsables de proteger sus credenciales de acceso al correo electrónico institucional y no deberán de compartirlas con terceros.

10.2. Todos los usuarios deben habilitar la autenticación en dos pasos (*2FA*) en sus cuentas de correo electrónico institucional. La *2FA* es obligatoria para acceder desde dispositivos no confiables o fuera de la red institucional. Esto añade una capa adicional de seguridad y reduce el riesgo de acceso no autorizado.

10.3. El uso de correo electrónico institucional se deberá limitar única y exclusivamente para asuntos relacionados con las actividades laborales.

10.4. Todo correo entrante de origen desconocido que contenga posible *spam*, correo no deseado, correo basura o información de dudosa procedencia debe ser ignorado y reportado a su enlace responsable de TIC o unidad análoga y en caso de no contar con este, con su proveedor de servicios de correos electrónico.

10.5. Será responsabilidad de cada usuario verificar que la información del correo electrónico sea la adecuada, revisando periódicamente la bandeja de entrada y salida.

10.6. Las personas servidoras públicas deberán tratar la información confidencial con la máxima seguridad. No deberán enviar información sensible sin cifrar, y no deben reenviar correos institucionales sin autorización previa.

10.7. Se deberán establecer procedimientos para la gestión segura de archivos adjuntos y enlaces en los correos electrónicos, incluyendo la prohibición de la apertura de archivos o enlaces desconocidos o no solicitados que puedan contener *malware.*

10.8. Se deberán definir períodos de retención para los correos electrónicos y establecer procedimientos para la eliminación segura de correos electrónicos obsoletos o no requeridos, en cumplimiento con las regulaciones de retención de registros.

10.9. Se deberán implementar herramientas de monitoreo y auditoría para supervisar el uso del correo electrónico, detectar actividades sospechosas y responder rápidamente a incidentes de seguridad relacionados con el correo electrónico.

11. POLÍTICA DE LA PLANEACIÓN DE INFRAESTRUCTURA EN RED.

11.1. De la infraestructura de red.

11.1.1. Se deberá establecer una topología de red jerárquica para optimizar la eficiencia y la escalabilidad. Esto incluirá la segmentación de la red en áreas funcionales para facilitar la administración y mejorar la seguridad.

11.1.2. La elección del equipamiento de red se debe guiar por estándares de la industria, considerando la capacidad actual y futura de la red.

11.1.3. Se deberán utilizar dispositivos de fabricantes reconocidos de las líneas empresariales por su confiabilidad y seguridad, con actualizaciones regulares de *firmware* y soporte.

11.1.4. Se deberá seguir los estándares de cableado que aseguren la confiabilidad y el rendimiento óptimo. Los cables se organizarán y documentarán adecuadamente, siguiendo normativas específicas para cada tipo de conexión.

11.1.5. La infraestructura de red deberá incorporar mecanismos de redundancia para mitigar posibles interrupciones.

11.1.6. Se deben implementar protocolos de tolerancia a fallos para garantizar una operación continua, incluso en situaciones de emergencia.

11.1.7. La actualización regular de *firmware* debe ser una práctica estándar para abordar y mitigar vulnerabilidades de seguridad potenciales, garantizando la integridad y confidencialidad de la información transmitida.

11.1.8. Se debe establecer un proceso estructurado para la implementación de cambios en la infraestructura de red, que incluirá la evaluación de impacto, la planificación detallada y la ejecución supervisada.

11.1.9. Se deben asignar responsabilidades específicas a los equipos involucrados, y se realizarán pruebas exhaustivas antes de la

implementación completa de una infraestructura de red.

11.1.10. Se deberá desarrollar un calendario de despliegue de una red que minimice el impacto en las operaciones de la entidad.

11.1.11. Se deberá contar con una red conmutada para la arquitectura de subred filtrada correspondiente a la zona desmilitarizada.

11.1.12. Se deberá contar con un enrutamiento estático entre los *routers* y la puerta de enlace de seguridad al momento de configurar una red.

11.1.13. No se deberá aceptar la información de enrutamiento de origen.

11.1.14. Solo se deberán instalar *software*/programas en la puerta de enlace de seguridad que sean absolutamente necesarios para la operación.

11.1.15. Se deberá asegurar de que los puertos no estén habilitados de forma predeterminada.

11.1.16. Se deberá asegurar de que los puertos del *Switch Port Analyzer* no estén habilitados a menos que se necesite el uso de sistemas de detección de intrusos.

11.1.17. Se deberá garantizar que las contraseñas que se implementen en las interfaces de los dispositivos cumplan con los requerimientos de una contraseña segura.

11.1.18. Se deberá asegurar que el registro de todos los eventos de administración y de todo el tráfico se encuentre habilitado para eventos de seguridad.

11.1.19. Se deberán establece procedimientos de seguridad claros que abarquen la autenticación, autorización, cifrado y auditoría de la infraestructura de red. Estos procedimientos se actualizarán regularmente para abordar las amenazas emergentes y garantizar un entorno seguro y conforme a los estándares.

11.1.20. Se implementarán controles de acceso basados en roles para limitar el acceso a la red y los recursos y lineamientos establecidos en la política de concesión y revocación de accesos.

11.2. Control de Redes.

11.2.1. Se deberán desarrollar procedimientos detallados para solicitar, revisar, aprobar e implementar cambios en la infraestructura de red. Cada solicitud de cambio será evaluada en función de su impacto potencial, con una atención especial a los cambios críticos que puedan afectar la seguridad, disponibilidad o rendimiento de la red.

11.2.2. Antes de la implementación, se deberá llevar a cabo una evaluación exhaustiva de impacto para comprender las implicaciones potenciales de cada cambio propuesto. Esto incluirá la identificación de posibles riesgos y la planificación de estrategias de mitigación.

11.2.3. Se deberán implementar sólo aquellos cambios autorizados, después de una evaluación de impacto completa de seguridad y rendimiento de la red.

11.2.4. Cada cambio deberá ser documentado de manera detallada, incluyendo la justificación, los pasos de implementación y cualquier lección aprendida. La documentación servirá como referencia futura y contribuirá a la mejora continua del proceso.

11.2.5. Se deberán establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

11.2.6. Se deberán proporcionar a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.

11.2.7. El área correspondiente de la administración de la infraestructura o área de TI deberá establecer el *software* correspondiente para monitorear la funcionalidad de las redes a través del uso de analizadores de red.

11.2.8. No se deberá realizar la instalación de dispositivos como puntos de acceso sin antes haber sido evaluada, autorizada, ejecutada y controlada por el área responsable de la infraestructura de red o área de TI. Esta medida se debe a que se vulnera la seguridad de la red y degrada el rendimiento de las conexiones afectando a todos los colaboradores de la entidad.

11.3. Seguridad de la Infraestructura de Red.

11.3.1. Se deberán establecer procesos regulares de auditoría para evaluar el cumplimiento de la infraestructura de red con las políticas de seguridad establecidas. Estas auditorías se realizarán de manera independiente y abordarán aspectos como la configuración de seguridad, el acceso autorizado y las actividades de registro.

11.3.2. Las acciones correctivas derivadas de auditorías se implementarán de manera oportuna y eficaz. Estas acciones podrían incluir ajustes en la configuración de seguridad, mejoras en la capacitación del personal o actualizaciones en las políticas y procedimientos para abordar las áreas identificadas de mejora.

11.3.3. Se deberán desplegar *firewalls* para filtrar el tráfico no autorizado, configurando reglas específicas para permitir únicamente el tráfico necesario para el funcionamiento de los servicios.

11.3.4. Se deberá contar con mecanismos de defensa tales como algún *Network Intrusion Detection (NIDS) y Network Intrusion Prevention (NIPS)* para la protección de la infraestructura.

11.3.5. Deberán implementarse mecanismos y procedimientos los cuales se encarguen de permitir, denegar o descartar conexiones o paquetes.

11.3.6. En caso de requerir acceso remoto a recursos de la entidad, se debe hacer uso de redes privadas virtuales (*VPN*), para ampliar la seguridad a través de túneles.

11.3.7. Se deberá implementar una lista de control de acceso (*VACL*) para controlar el acceso hacia y desde las *VLAN*. Se deberán crear filtros *VACL* para denegar a los paquetes la capacidad de fluir a otras *VLAN*.

11.3.8. Se deberán deshabilitar los protocolos de administración remota sin cifrar que se utilizan para administrar la infraestructura de red (verbigracia *Telnet*, Protocolo de transferencia de archivos [*FTP*]).

11.3.9. El enlace responsable de TIC o unidades análogas deberá deshabilitar los servicios innecesarios, o en su caso solicitarlo a la DGGD.

11.3.10. Para la administración y control de las configuraciones en servidores se deberá configurar el acceso seguro a las líneas de consola, auxiliares y terminales virtuales.

11.4. Segmentación de redes.

11.4.1. Se deberán identificar y definir claramente los segmentos de red con base en criterios de seguridad y funcionalidad. Esto incluirá la separación de redes para diferentes departamentos, niveles de confidencialidad y tipos de tráfico, garantizando una adecuada segmentación para limitar la propagación de posibles amenazas.

11.4.2. Se deberán establecer procedimientos de acceso que regulen la comunicación entre diferentes segmentos de red. Estos procedimientos se basarán en el principio de mínimo privilegio, restringiendo el tráfico solo a lo esencial para las operaciones y limitando la exposición potencial a amenazas internas.

11.4.3. Se deberán establecer sistemas de monitoreo continuo para supervisar el tráfico entre segmentos. Cualquier actividad inusual o no autorizada se identificará rápidamente, permitiendo una respuesta inmediata para mitigar posibles amenazas y garantizar la seguridad global de la red.

11.4.4. Se deberá hacer uso de *VLANs* para separar lógicamente el tráfico en una red física, definiendo reglas de *VLAN* que reflejen los requisitos de segmentación.

11.4.5. Se deberá contar con una gestión y administración de la red fuera de banda (*OOB*).

11.4.6. Se deberá usar enrutamiento y reenvío virtual (*VRF*) para segmentar el tráfico de red en múltiples tablas de enrutamiento simultáneamente en un solo *router*.

11.5. Infraestructura física.

11.5.1. Es responsabilidad del área encargada de la infraestructura de red velar por la integridad de esta, por lo cual su mantenimiento sólo puede ser hecho por personal especializado y bajo supervisión. Todos los requerimientos de nuevas conexiones de redes deben ser dirigidos a los responsables de la red.

11.5.2. Se deberán implementar medidas para restringir el acceso físico a las instalaciones que albergan la infraestructura de red. Esto incluirá sistemas de control de acceso, cámaras de vigilancia y registros de entrada, asegurando que solo personal autorizado tenga acceso a áreas críticas.

11.5.3. Se deberán implementar sistemas de respaldo de energía para garantizar el funcionamiento continuo de la infraestructura de red en caso de cortes de energía. Estos sistemas pueden incluir generadores de respaldo y baterías para asegurar la disponibilidad constante de los servicios críticos.

11.5.4. Se deberá reforzar los dispositivos de red haciendo uso de las configuraciones seguras establecidas por la entidad.

11.5.5. Se deberá establecer sistemas de monitoreo ambiental para supervisar las condiciones físicas en las instalaciones. Esto incluirá la detección de cambios en la temperatura, humedad y otros factores que puedan afectar negativamente la infraestructura de red, permitiendo una respuesta proactiva antes de que se produzcan problemas graves.

11.5.6. El cableado se deberá organizar de manera estructurada y se deberá etiquetar claramente para facilitar la identificación y el mantenimiento. La documentación detallada de la disposición física del cableado permitirá una rápida intervención en caso de problemas y facilitará futuras expansiones o modificaciones.

11.5.7. Para la administración de las funciones de red, deberán ser realizadas desde un *host* dedicado y totalmente parcheado a través de un canal seguro, preferiblemente *OOB*.

11.6. Protección de Redes inalámbricas.

11.6.1. Para el proceso de adquisición de un punto de acceso inalámbrico, se deberá cambiar las contraseñas predeterminadas por el proveedor del servicio.

11.6.2. Los responsables de la infraestructura de red deberán sólo permitir acceso a la red al colaborador autorizado.

11.6.3. La red deberá estar cifrada por *WPA2 y WPA3.*

11.6.4. Se deberá proteger el identificador de la red *(SSID)*, cambiarlo por uno único para evitar la identificación del recurso.

11.6.5. Se deberá realizar la configuración de un *Firewall* en los dispositivos inalámbricos (*Firewall* basado en *host*) así como para la red interna (*Firewall* basado en enrutador o módem).

11.6.6. Los responsables de la infraestructura de red deberán mantener el *software* de punto de acceso parcheado y actualizado.

11.6.7. Se deberá considerar el uso de un portal de acceso para validar la autenticación a redes inalámbricas e impedir el acceso a recursos críticos de la red.

11.7. Filtrado de paquetes.

11.7.1. Se deberán implementar *firewalls* perimetrales para filtrar el tráfico entrante y saliente en los límites de la red. Estos *firewalls* serán configurados para permitir únicamente el tráfico autorizado, bloqueando cualquier intento no autorizado de acceso a la red.

11.7.2. Se deberán establecer reglas específicas para el filtrado de paquetes, definiendo qué tipos de tráfico son permitidos o bloqueados en función de criterios como dirección *IP*, protocolo, puertos y patrones de tráfico. Estas reglas serán revisadas y actualizadas regularmente para adaptarse a las necesidades cambiantes de seguridad.

11.7.3. Se deberán implementar soluciones de filtrado de contenido para bloquear el acceso a sitios web maliciosos o inapropiados. Esto se logrará mediante la inspección de los datos en el nivel de aplicación, identificando y bloqueando contenido no deseado según políticas establecidas.

11.7.4. Como mínimo, el dispositivo de filtrado de paquetes deberá ser capaz de:

a) Soportar el filtrado de paquetes sobre la base de (paquete). Dirección IP de origen y de destino;

b) Puerto de origen y destino (para TCP, UDP);

c) Dirección de la conexión (entrante, saliente);

d) Preservar las reglas de filtrado como inherentemente consistentes;

e) Filtrar paquetes para cada interfaz de red por separado;

f) Soporte de paquetes de multidifusión si se necesita agrupamiento de dispositivos;

g) Preservar el orden de las reglas de filtrado por la pasarela de seguridad;

h) Limitar la longitud de los fragmentos de los paquetes IP y definir un desplazamiento mínimo de fragmentos;

i) Filtrar los mensajes ICMP destino inalcanzable y redireccionar; y,

j) Evitar la suplantación de direcciones IP internas si provienen de Internet (debido a la suplantación de IP).

12. POLÍTICA DE LA CONCIENTIZACIÓN Y MITIGACIÓN DE RIESGOS EN TEMAS DE CIBERSEGURIDAD.

12.1. Se deberá adoptar como medida preventiva y de generación del conocimiento los distintos temas de Ciberseguridad aplicables a usuarios que manejen información, aplicativos, cuentas de correo electrónico institucionales, equipos de cómputo y móviles. Dichos temas deberán incluir al menos lo siguiente:

a) Campañas de concientización; y,

b) Estrategias de generación de conocimiento respecto a los temas que relacionan las amenazas y riesgos entorno a la ciberseguridad.

12.2. Los cursos de capacitación deberán incluir temas referentes a la protección contra riesgos de ciberseguridad relevantes en el momento de la realización del curso, así como los riesgos más comunes. En términos de periodicidad, lo ideal será que sean impartidos al menos una vez cada año.

12.3. La distribución de información con respecto a dichos cursos/capacitaciones deberán ser comunicada a través de medios oficiales, de tal manera que pueda llegar de manera adecuada a todas las personas que les correspondan participar en las mismas.

12.4. Se deberán realizar evaluaciones de competencias (o a manera de sondeo) para identificar las áreas en las que el personal colaborador requiere desarrollo de habilidades y mayor conciencia de seguridad.

12.5. De acuerdo con las áreas de oportunidad identificadas, se deberán utilizar una combinación de métodos de formación que se adapten para un mejor entendimiento de los colaboradores; tales como cursos presenciales, seminarios, formación en línea, simulaciones, entre otros.

DISPOSICIONES TRANSITORIAS

Primera.- Las presentes Políticas de Ciberseguridad entrarán en vigor a partir del día siguiente de su publicación en el Periódico Oficial del Gobierno Constitucional del Estado de Michoacán de Ocampo.

Segunda. - Las cuestiones operativas no previstas serán atendidas en el ámbito de su competencia por la Dirección General de Gobierno Digital.

Tercera.- Las presentes Políticas podrán ser actualizadas de conformidad a la innovación, modificación de funciones, atribuciones y necesidades de la administración pública.

Morelia Michoacán, a 09 de octubre de 2024.

A T E N T A M E N T E

L.A.E. LUIS NAVARRO GARCÍA
SECRETARIO DE FINANZAS Y ADMINISTRACIÓN
(Firmado)

M. EN D.A. JUAN PAULO GRANADOS GÓMEZ
DIRECTOR GENERAL DE GOBIERNO DIGITAL
(Firmado)