Política de Seguridad de la Información.

CONTROL DE VERSIONES DEL DISEÑO DEL DOCUMENTO				
No.	**Fecha**	**Descripción del Cambio**	**Responsable**	**Versión**
1	Junio 2022	Elaboración del documento.	Lic. María del Consuelo Reyna Lara	1.0
2	Enero 2024	Actualización del Documento	Lic. María del Consuelo Reyna Lara	1.1

MARCO NORMATIVO

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. **DOF: 06/09/2021**

CAPÍTULO VI, SEGURIDAD DE LA INFORMACIÓN

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

Artículo 76.- El MGSI deberá conformarse, al menos por los siguientes elementos:
a) El establecimiento de objetivos alineados a la política general de seguridad de la información;
b) La identificación de los procesos y activos esenciales de la Institución, a través de un diagnóstico que involucre a las áreas que participan en la gestión de la información;
c) Elaboración de un análisis de riesgos para identificar las amenazas y vulnerabilidades;
d) La implementación de los controles mínimos de seguridad de la información, con base enla clasificación de los activos de información institucionales, y de conformidad con los Estándares Técnicos de la CEDN;
e) Programa de gestión de vulnerabilidades, que incluya su identificación, evaluación y corrección. La identificación de las mismas deberá partir de un análisis de vulnerabilidades al interior de la Institución, así como de las alertas o investigaciones de seguridad divulgadas por fuentes externas;
f) Un protocolo de respuesta ante incidentes de seguridad de la información, que contemple la conformación de un Equipo de Respuesta a Incidentes de Seguridad de la Información(ERISC), acciones de preparación, detección y análisis, contención, erradicación y recuperación, así como actividades posteriores al incidente, de conformidad con el Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
g) Plan de continuidad de operaciones y plan de recuperación ante desastres que consideren los aspectos para el restablecimiento de la operación de TIC, la información y los servicios;

h) Los mecanismos de supervisión y evaluación que permitan medir la efectividad de los controles de SI y de madurez institucional en la gestión de SI;

Lo anterior, con base en procesos de planeación, implementación, supervisión y mejora continua. Con la información y documentos generados, la UTIC deberá completar la información requerida a través de la Herramienta en la sección correspondiente al MGSI.

Artículo 77.- En cada Institución, la persona titular de la UTIC tendrá el rol de Responsable de la Seguridad de la Información (RSI), a excepción de las Instituciones que por su legislación específica o estructura organizacional cuenten con un área de Seguridad de la Información que no dependa de la UTIC, en dichos casos el rol de Responsable recaerá en la persona titular del área de Seguridad de la Información.

Artículo 78.- El RSI creará grupos de trabajo para la definición, implementación y evaluación del MGSI, los cuales se conformarán por la persona titular de la UTIC, los servidores públicos involucrados en la operación institucional y procesos relacionados con la seguridad de la información, y el RSI cuando este rol no recaiga en la persona titular de la UTIC. Cada grupo de trabajo documentará sus objetivos, actividades y definirá los roles de los servidores públicos que formen parte del mismo.

Artículo 79.- El RSI, tendrá entre otras, las siguientes responsabilidades:
I. Dar seguimiento a la conformación del MGSI, así como a su implementación y al cumplimiento de los controles mínimos de seguridad;
II. Presentar a sus superiores jerárquicos, incluido el titular de la Institución, un informe sobre la integración del MGSI, con la finalidad de comunicar su contenido y mecanismos de ejecución. En la presentación deberá considerarse la presencia de la persona titular de la UTIC cuando el rol de RSI no recaiga en éste;
III. Dar aviso inmediato a la CEDN sobre los incidentes de seguridad de la información que se presenten, y asegurarse del cumplimiento del Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos;
IV. Implementar un programa de evaluaciones, que contemple al menos, una evaluación trimestral del MGSI para verificar el desempeño de los controles de seguridad y determinar acciones de mejora;
V. Hacer del conocimiento del OCF en la institución y/o de las autoridades competentes, las irregularidades u omisiones en cumplimiento del MGSI, o delitos relacionados con la seguridad de la información en que incurran las personas servidoras públicas, y en su caso los proveedores y su personal, obligados a su observancia; así como
VI. Mantener un proceso de mejora continua del MGSI para cumplir con las disposiciones aplicables.

Artículo 80.- En aquellos casos en que la Institución requiera, para su operación y adecuada implementación del MGSI, efectuar una contratación para la adquisición, arrendamiento o prestación de servicios en materia de SI, dicha contratación deberá ser justificada y realizarse de conformidad con el proceso de planeación y dictamen que se detallan en los Títulos Segundo y Tercero de este Acuerdo.

Artículo 81.- El proceso de mejora continua del MGSI será revisado por la CEDN bajo las siguientes directrices:

I. En enero y julio de cada ejercicio, la Institución deberá actualizar en la Herramienta, la documentación del MGSI, e incorporar, adicionalmente, un informe que contenga el resultado de las evaluaciones efectuadas a los controles de seguridad y la descripción de las acciones de mejora implementadas en el último semestre;

II. Dicha información será revisada por la CEDN, que podrá emitir en cualquier momento, las observaciones que considere pertinentes, otorgando a las Instituciones, un plazo de hasta 15 días para solventarlas;

III. La CEDN podrá sugerir a las Instituciones la realización de evaluaciones técnicas adicionales, así como su colaboración para efectuarlas, con la finalidad de favorecer los máximos umbrales posibles en la eficacia del MGSI; así como

IV. Las recomendaciones que emita la CEDN deberán ser atendidas por la Institución.

INTRODUCCIÓN

La seguridad de la información es el seguimiento a un plan de acciones enfocadas a resguardar la confidencialidad, integridad y disponibilidad de los servicios, datos, documentos e información, la componen puntos básicos de la seguridad de la información, y tiene como meta establecer ciertos requerimientos para proteger la información de los usuarios de la institución de oficinas centrales como direcciones de enlace técnico, los servicios y equipos tecnológicos. Esta Política de Seguridad es de suma importancia para la institución, es un conjunto de requerimientos, directrices y protocolos que debemos seguir en materia de seguridad de la información. Deberá ser desarrollo por normas de uso, estándares normativos, procedimientos, y buenas prácticas, etc.). En esta época las tecnologías de la información sufren un gran número de amenazas y peligros, por lo cual se necesita un esfuerzo por adaptarse y solucionar los riesgos que tienen estas.

OBJETIVO

El objetivo de la política de la seguridad es la información, es precisar los puntos básicos para la gestión de la seguridad de la información, la misión es lograr que la Subdirección de Recursos Humanos y TIC's garantice la seguridad de la información y los servicios, así como minimizar los riesgos y amenazas; así como establecer las políticas para la protección de la información: recursos, instalaciones y equipos asociados con su procesamiento, mantener la continuidad del negocio, previniendo y minimizando los incidentes de seguridad que se presentan en las áreas de la CONAZA.

ALCANCE

Este documento es de aplicación obligatoria para todo el personal de las diferentes áreas, unidades y proveedores de la CONAZA, considerando que las prácticas de seguridad se realizarán de forma constante y sistemática y deberán cubrir todos los ámbitos de seguridad física y lógica, la política se aplica para las Oficinas Centrales y las Direcciones de Enlace Técnico de la CONAZA. El alcance abarca toda la información de la institución y quién acceda a ella, a los equipos tecnológicos que contengan información y el lugar en el que se encuentre, ya se trate de información impresa, digitalizada o almacenada electrónicamente en algún dispositivo. Esta política se enfoca a todas las áreas, y deberá ser conocida por todo el personal de la institución.

RESPONSABILIDADES

Del Documento:

- El área de TIC's y la Dirección de Administración de la CONAZA, aprueba la presente Política y apoyará a la Subdirección de Recursos Humanos y TIC's para el cumplimiento de la misma.
- La Subdirección de Recursos Humanos y TIC's es responsable de hacer de conocimiento para su aprobación y dar seguimiento al cumplimiento de la misma, por parte de las áreas involucradas.
- El Departamento de TIC's es responsable de asegurar que este documento sea revisado de acuerdo con los requerimientos del MGSI.

De la Política:

- El personal adscrito a las Unidades Administrativas de la CONAZA serán los responsables de dar cumplimiento a las políticas establecidas en el presente documento.
- La Subdirección de Recursos Humanos y TIC's, es responsable de implementar, mantener y operar los controles de seguridad aplicables que son mencionados en la presente política.
- El responsable de la seguridad de la Información, es responsable de supervisar que los responsables de implementar controles de seguridad del MGSI y controles para el manejo

de riesgos, lleven a cabo su tarea en tiempo y forma, con apego a la definición del control de seguridad correspondiente.

- El responsable de seguridad de la información debe establecer una política de seguridad de la información, que vaya en línea con la visión, misión, y los valores de acuerdo con las necesidades de la CONAZA.
- La política deberá quedar aprobada por la Dirección de Administración.
- Como medio oficial se entienden, comunicados, documentos, oficios, correo electrónico o cualquier evidencia que pueda ser trazada o documentada en cualquier medio.
- La política quedará formalmente documentada en la estructura del Marco de Gestión de Seguridad de la Información (MGSI) de la CONAZA.
- Los usuarios son responsables de la implementación de los lineamientos establecidos en la presente política.
- Se considera incumplimiento a toda acción que contravenga lo estipulado en estas políticas y a cualquier acción deliberada y sin autorización que dañe o corrompa el desempeño normal, o cause, el mal funcionamiento de equipos, sistemas y servicios de la CONAZA.

DECLARACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La CONAZA, en su transformación se plantea la misión de contribuir para resolver el problema de las comunidades rurales de zonas áridas con acciones de conservación de agua, suelo y cubierta vegetal a fin de apoyar a la sustentabilidad alimentaria y productiva. Con atención particular de los productores sociales que habitan en el mas del 60% y 70% del territorio nacional, el cual son zonas áridas y en proceso de degradación, Fortaleciendo las unidades de producción rural, integración a las cadenas de producción y así incrementar su condición económica, proyectando a los beneficiarios para mejorar su calidad de vida, esto a través del Proyecto Estratégico Establecimiento de Parcelas de Nopal Forrajero y Estimulación de Lluvias ante el Estrés Hídrico en Zonas Áridas de México.
La Subdirección de Recursos Humanos y TIC's tomará las acciones correspondientes para regular y asegurar el debido cumplimiento para la protección de la información, así como de los recursos tecnológicos en los que dicha información se genera, almacena, utiliza y/o dispone, con el fin de contribuir con el entorno confiable que requiere en esta materia la CONAZA para el debido cumplimiento de sus objetivos.

Esta estrategia se llevará a cabo con la implementación políticas, controles de seguridad, tecnologías y procedimientos que permitan detectar cualquier tipo de amenaza y/o vulnerabilidades. Estos procedimientos serán el eje rector para todo el personal que tengan acceso a información y a los activos utilizados para su consulta, procesamiento,

almacenamiento y/o transmisión, permitiendo con esto concientizar a los usuarios sobre los aspectos de seguridad de la información, definir perfiles para el uso de servicios y aplicaciones, reforzar la seguridad en los sistemas, promover el respaldo de información y brindar seguridad física en la información, entre otros, tomando como base los principios rectores de protección:

- **Confidencialidad:** La garantía de que la información no será revelada por individuos, programas o procesos no autorizados.
- **Integridad:** La información debe ser exacta, completa y protegida de modificaciones no autorizadas o inesperadas.
- **Disponibilidad:** La información, los sistemas y los recursos deben estar disponibles a los usuarios autorizados en forma oportuna.

Todo esto atreves de controles, administrativos, técnicos y físicos.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONAZA

La seguridad de la información se logra a través de la implementación de un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos y por supuesto herramientas de software y hardware. Estos controles necesitan ser establecidos, implementados, revisados y mejorados, cuando sea requerido, para garantizar que la seguridad información, se debe llevar a cabo lo siguiente:

- La política debe quedar formalmente aprobada por la Dirección de Administración, su vigencia será permanente a menos que existan cambios que requieran una nueva versión del documento.
- El Departamento de Tecnologías de la Información revisará por lo menos dos veces al año la adecuación y suficiencia de la política de seguridad de la información, con respecto a las necesidades de la CONAZA en materia de seguridad de la información.
- Cualquier cambio en la política debe quedar aprobado por la Dirección de Administración.
- Cada vez que exista una nueva publicación, el número de la versión de la política general de seguridad de la información será controlado.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Se deben otorgar las facultades generales o específicas al personal de TIC's, preservando una adecuada segregación y delegación de funciones, así como sus restricciones.
- Se debe delimitar las facultades entre el personal que autorice, ejecute, vigile, evalúe, registre y contabilice las transacciones.
- Los responsables de los procesos en cada Unidad Administrativa de la CONAZA deben asegurar que las tareas y responsabilidades sean debidamente segregadas con el fin de evitar las oportunidades de modificaciones a la información contenida en la infraestructura esencial de la CONAZA de forma no autorizada, sean intencionales o accidentales.
- Los perfiles definidos y autorizados por los responsables de los procesos deberán configurarse conforme a las restricciones de cada aplicación por el personal de cada Unidad Administrativa.
- Las Unidades Administrativas deben seguir lo establecido en la Política para reducir el riesgo de mal uso accidental o deliberado de los servicios de TIC e infraestructura esencial de la CONAZA.

SEGURIDAD EN LOS RECURSOS HUMANOS

Para asegurar que los empleados y los proveedores entiendan sus responsabilidades y que son los adecuados para los roles que son considerados, se deben seguir las siguientes políticas:

- Todos los empleados de las Unidades Administrativas, o en su caso, personal externo que presta algún tipo de servicio a la Institución, deben recibir el entrenamiento apropiado respecto al tema de la seguridad de la información en el que se incluya la instrucción sobre las políticas, prácticas y procedimientos vigentes, las responsabilidades y obligaciones particulares, los requerimientos legales en esta materia, la forma de minimizar riesgos y las consecuencias de no acatar la normatividad establecida.
- Todo esto con la finalidad de fomentar una cultura de trabajo orientada a la unificación de criterios y al reforzamiento del comportamiento esperado de los empleados sobre la importancia de la seguridad de la información y sus obligaciones para reducir errores humanos y evitar abusos en el manejo de los bienes de información y sistemas asociados.

- El personal que está directamente relacionado con la administración de la seguridad deberá tener el conocimiento y estar capacitado en lo referente al tema.
- Es responsabilidad y obligación de todo empleado de la CONAZA; mantenerse informado de las normas, disposiciones y prácticas de seguridad de la información que dicta la CONAZA.
- Definir en el documento Programa de concientización y capacitación en seguridad de la información los productos que se generarán durante el año, estableciendo los pasos para su realización, las fechas de inicio y termino, recopilación de evidencia y responsable de su desarrollo.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

- Queda prohibido instalar software sin la autorización del área de TIC's, para ello, el área requirente deberá solicitar y justificar mediante correo electrónico dirigido al a la Subdirección de Recursos Humanos y TIC's y al Departamento de TIC's el software que requiere instalar.
- Los anteriores dictaminarán si es procedente la instalación de cualquier software.
- Todos los equipos de cómputo de la CONAZA deberán tener un programa autorizado de antivirus actualizado y activado.
- Todos los dispositivos de almacenamiento interno o externo con información deberán ser revisados antes de ser utilizados con el software de antivirus.
- Queda prohibido descargar software o programas de internet sin la autorización del área de TIC's, así como cualquier archivo de música, video o fotográfico que no se encuentre plenamente justificado como parte de las funciones de la persona.
- Queda prohibido cambiar la configuración o parámetros de los equipos de cómputo, sistemas operativos o aplicaciones de la dependencia, sin la autorización del área de TIC's que podría exponer la información de los equipos a riesgos no identificados.

SEGURIDAD EN LAS REDES

- El uso del servicio de Internet en la CONAZA debe contar con herramientas de seguridad y de filtrado de contenido, los cuales deben ser definidos por el área de TIC's.
- Las conexiones a la red de equipos externos serán verificadas por el área de TIC's para validar su conexión a la red local.

VULNERABILIDADES TÉCNICAS

- Se debe de contar con información acerca de las vulnerabilidades técnicas de los sistemas y aplicaciones que están en operación en la CONAZA, evaluar las vulnerabilidades y tomar las medidas apropiadas para manejar los riesgos asociados.
- Una vez que se ha identificado una nueva vulnerabilidad técnica, se deben identificar los riesgos asociados y las acciones a ser tomadas.
- Dependiendo de qué tan urgente sea la vulnerabilidad técnica, las acciones a tomar deben llevarse a cabo y regístralo en la bitácora de vulnerabilidades.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades, se deben seguir los siguientes lineamientos:

- El ERISC será el encargado de coordinar la recepción y seguimiento de los incidentes de seguridad.
- Todo incidente debe ser registrado en el repositorio de seguridad de la información.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La CONAZA deberá nombrar a un responsable para la administración de la continuidad de las operaciones en caso de un desastre o falla mayor, el responsable deberá considerar lo siguiente:

- Entender los riesgos del negocio, su probabilidad e impacto.
- Identificar la prioridad que tienen los procesos críticos del negocio.
- Coordinar esfuerzos de todas las áreas operativas y de soporte.
- Formular y documentar la estrategia del Plan de Recuperación de Desastre.
- Formular y documentar los planes de continuidad alineados con la estrategia de recuperación.
- Realizar pruebas y actualizaciones del proceso, los planes y los procedimientos de continuidad.
- El responsable del plan de continuidad debe considerar una estrecha comunicación con las áreas operativas, tecnológicas y Protección Civil.
- Es indispensable llevar a cabo un Análisis de Impacto al Negocio a partir del cual se identifiquen los eventos que pueden causar interrupciones a los procesos de negocio

y los requerimientos de recuperación en función de las prioridades del negocio y del impacto que pudieran provocar. Esta evaluación considera todos los procesos de las Unidades Administrativas y no está limitado solo al área de tecnologías de información.

- Los planes deberán ser desarrollados para mantener o restaurar la operación de las actividades críticas de la Dependencia, en las escalas de tiempo requeridas después de que se haya presentado una interrupción, falla o desastre.

EL PROCESO DE PLANEACIÓN DE LA CONTINUIDAD DEL NEGOCIO DEBE CONSIDERAR

1. Identificación y acuerdo de todas las responsabilidades y procedimientos de emergencia.
2. Implantación de los procedimientos de emergencia necesarios para la recuperación y la restauración en las escalas de tiempo requeridas.
3. Documentación y formalización de los procesos y los procedimientos.
4. Directorio de datos de personal clave que incluya al menos teléfono y celular.
5. Prueba y actualización de los planes.

CUMPLIMIENTO LEGAL

La presente política aplica a toda área que por sus responsabilidades esté llamada a cumplir con algún requerimiento en materia de seguridad de la información y que sea sujeto de auditorías o evaluaciones en materia de seguridad de la información.

La CONAZA deberá tener perfectamente identificados y documentados los requisitos legales que en materia de seguridad de la información debe cumplir. Los controles específicos y las responsabilidades individuales para atender las obligaciones deben ser definidos y documentados también.

En caso de ser necesario, la Dirección Jurídica debe proveer asesoría en la identificación de estas obligaciones legales.

Se debe apegar a lo estipulado en la Ley de Transparencia y Acceso a la información Pública Gubernamental, en el caso de que sea requerida la privacidad de la información que regule a alguna actividad de la CONAZA, ésta deberá estudiar a fondo los requerimientos legales que debe cumplir para implantar los mecanismos de control que garanticen la privacidad de la información sensible que custodian terceros.

El área Jurídica de la CONAZA deberá brindar asesoría en la interpretación de las obligaciones legales en esta materia.

REVISIONES AL MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Para mejorar la eficiencia de los controles de seguridad, su cumplimiento debe ser monitoreado continuamente. Por lo cual se deben realizar revisiones periódicas que permitan identificar las mejoras de manera oportuna para evitar brechas de seguridad de la información.
- Se debe asegurar que la revisión se lleve a cabo por personal que no haya participado en el diseño o implementación de los controles o que pertenezca a las áreas evaluadas, el personal puede ser interno o externo.
- Las revisiones internas deben realizarse al menos una vez al año y se deben realizar en las áreas y/o procesos relevantes de la CONAZA, así como en aquellos especialmente débiles que se pudieran haber detectado en revisiones previas (internas o externas).
- Los resultados de las revisiones independientes deben ser resguardadas y reportadas al área de TIC's.
- Estas revisiones solo podrán ser llevadas a cabo bajo la supervisión y autorización de la Subdirección de Recursos Humanos y TIC's siguiendo los siguientes lineamientos:
  -Planear los requerimientos para la revisión.
  -Delimitar el alcance de la revisión.
  -Identificar las herramientas de apoyo.
  -Registrar y monitorear las actividades de la revisión.
  -Documentar y presentar los hallazgos en tiempo y forma.

ADMINISTRACIÓN DE RIESGOS

Equipo de Trabajo para el Análisis de Riesgos se encargará de la Administración de los riesgos de la información, asociada con las estrategias, procesos y actividades de la CONAZA.
La Unidad de Administración y Finanzas deben participar en la identificación, evaluación y monitoreo periódico de los riesgos, la cual en conjunto con el área afectada definirá el impacto económico que podrían traer, así como la inversión para combatirlos.
Todos los riesgos de la información identificados en la CONAZA deben tener un monitoreo, seguimiento y control para minimizarlos o eliminarlos, mismos que se registrarán en la bitácora de riesgos de seguridad de la información.
El análisis de riesgos de seguridad de la información se realizará mínimo cada año, o cuando exista un cambio significativo en la CONAZA, con forme al Proceso de Gestión de Riesgos.
El análisis de riesgos de seguridad de la información debe dar cumplimiento a la normatividad aplicable en tecnologías de la información.

PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.
Se deberá cumplir lo establecido en la Ley General de protección de Datos Personales en posesión de Sujetos Obligados atendiendo los principios de:

- Licitud.
- Finalidad.
- Lealtad.
- Consentimiento.
- Calidad.
- Proporcionalidad.
- Información.
- Responsabilidad.
- Seguridad de la información - Medidas físicas.
- Seguridad de la información - Medidas administrativas.
- Seguridad de la información - Medidas técnicas.
- Confidencialidad, integridad y disponibilidad.
- Derechos ARCO.
- Resultado de la evaluación de impacto o justificación para su no elaboración.

- La Unidad de Transparencia de la CONAZA apoyará en actividades referente a la materia de protección de datos personales y a lo referente al Art. 30 de la LGPDPPSO.

- Se deberá publicar en cada aplicación y/o sistema que reciba datos personales, avisos de privacidad integral, simplificada, así como aviso de consentimiento y aceptación de uso y tratamiento de la información, en caso de requerir apoyo, o exista alguna duda o comentario, se podrá solicitar la intervención de la Unidad de Transparencia.

SANCIONES

- Cada vez que sea detectado un incumplimiento a las políticas y controles de seguridad de la CONAZA se debe evaluar la influencia de fallas tecnológicas o administrativas, para determinar los hechos como circunstanciales.
- Se considera incumplimiento a toda acción que contravenga lo estipulado en estas políticas y a cualquier acción deliberada y sin autorización que dañe o corrompa el desempeño normal, o cause, el mal funcionamiento de equipos, sistemas y servicios de la CONAZA.
- Se considera reincidencia a las acciones efectuadas más de una vez, independientemente de que su ocurrencia sea consecutiva inmediata o después de un lapso indeterminado.
- Las reincidencias se tratarán indistintamente, ya sea un caso involuntario o intencional.

Una vez detectado un incidente de incumplimiento, proceden las siguientes instancias básicas de acción:
1) Nivel 1. Recomendación personal, individual y sin consecuencias administrativas o marcas en el expediente del empleado.
2) Nivel 2. Recomendación personal, con notificación a sus jefes inmediatos.
3) Nivel 3. Última llamada de atención con la notificación al jefe inmediato, indicando que se levantará un acta administrativa en la siguiente llamada.
4) Nivel 4. Exhortación correctiva con notificación a sus jefes inmediatos, con levantamiento de acta administrativa correspondiente solicitando a las autoridades competentes la inclusión la falta en el expediente del empleado.

Sólo la unidad responsable de dichas atribuciones puede imponer las siguientes acciones de acuerdo con la gravedad de cada caso:
1) En caso de ser la tercera llamada de atención por la violación de las políticas, un incidente de incumplimiento o mal uso del servicio o contraseña de acceso, se llevará a cabo la cancelación temporal inmediato y sin previo aviso.
2) En caso de ser la última llamada de atención, se llevará a cabo la cancelación definitiva inmediata y sin previo aviso de la contraseña o servicio.
3) Exhortación correctiva con notificación a sus jefes inmediatos, con levantamiento de acta administrativa correspondiente solicitando a las autoridades competentes, así como la inclusión de la falta en el expediente del empleado.

REFERENCIAS

• **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 seguridadde la información en la Administración Pública Federal.
DOF: 06/09/2021.

• **LGPDPPSO.** Ley General de protección de Datos Personales en posesión de Sujetos Obligados.
DOF: 26/01/2017.

ELABORACIÓN, REVISIÓN, APROBACIÓN DEL DOCUMENTO

RESPONSABLE DE LA ELABORACIÓN, REVISIÓN Y APROBACIÓN DE LA PRESENTA POLÍTICA		
ELABORACIÓN	**REVISIÓN**	**APROBACIÓN**
Lic. Abies Alejandro Lom Malacara Jefe del Departamento de TIC's	**Lic. María del Consuelo Reyna Lara** Subdirectora de Recursos Humanos y TIC's	**Lic. José Manuel Gutiérrez Saucedo** Director de Administración