



# Instituto Nacional de Estadística

## POLÍTICA INSTITUCIONAL

### Fundamento de Ley:

Normas Generales y Técnicas de Control Interno Gubernamental,  
Acuerdo A-039-2023 de la Contraloría General de Cuentas



**INSTITUTO NACIONAL DE ESTADÍSTICA**  
**RESOLUCIÓN DE GERENCIA No. 187-2025**

Guatemala, 29 de diciembre de 2025

**CONSIDERANDO**

Que el Instituto Nacional de Estadística, es una Institución con carácter de entidad estatal, descentralizada, semiautónoma, con personalidad jurídica, patrimonio propio y plena capacidad para adquirir derechos y contraer obligaciones que tiendan al desarrollo de sus fines y de conformidad con el artículo catorce (14) de la Ley Orgánica del Instituto Nacional de Estadística, Decreto Ley tres guion ochenta y cinco (3-85), el Gerente es el Jefe Superior de las Unidades Administrativas y Técnicas del INE y responsable ante la Junta Directiva por el correcto y eficaz funcionamiento de la Institución.

**CONSIDERANDO**

Que la Junta Directiva mediante Resolución JD guion diecisiete diagonal veinte diagonal trece (RESOLUCIÓN JD-17/20/13) de fecha veinticuatro (24) de julio de dos mil trece (2013), estableció dentro de las atribuciones del Gerente del Instituto Nacional de Estadística, la de aprobar y modificar Manuales Administrativo-Operativos que contengan los mecanismos y procedimientos de procesos internos, que sirvan de apoyo al funcionamiento Administrativo y Técnico de la Institución, asimismo en la Resolución JD INE número quince guion veintidós guion dos mil diecinueve (RESOLUCIÓN JD INE No. 15-22-2019) de fecha dieciocho (18) de julio de dos mil diecinueve (2019), que contiene el Reglamento Orgánico Interno -ROI- del Instituto Nacional de Estadística, en su artículo cuarenta y ocho (48) contempla lo relacionado a los Manuales Administrativos, en donde el Gerente del Instituto Nacional de Estadística queda facultado para aprobar Manuales Administrativos orientados a coadyuvar el adecuado funcionamiento y organización de las Unidades Administrativas y Técnicas que conforman la Institución.

**CONSIDERANDO**

Que el Director de Informática del Instituto Nacional de Estadística, por OFICIO DI-419-2025, trasladó el documento que contiene la **“Política Institucional de Seguridad y uso de Tecnologías de la Información” Versión 2**, que establece lineamientos que orientan el uso adecuado, seguro y responsable de los sistemas, equipos y servicios informáticos institucionales, asegurando la protección de la información estadística y administrativa que se genera, procesa y resguarda en el INE, previamente revisado por la Dirección de Planificación de esta institución, para dar apoyo en el cumplimiento de la norma número cuatro “Normas Aplicables a la Información y Comunicación” del Acuerdo Número A guion cero treinta y nueve guion dos mil veintitrés (A-039-2023), Normas Generales y Técnicas de Control Interno Gubernamental de la Contraloría General de Cuentas y la Ley de Acceso a la Información Pública, Decreto cincuenta y siete guion dos mil ocho (57-2008) del Congreso de la República de Guatemala.

**POR TANTO**

El Gerente del Instituto Nacional de Estadística, en el uso de las facultades que la Ley le otorga y de conformidad con el artículo diecisiete (17) numerales uno (1) y quince (15) de la Ley Orgánica del Instituto Nacional de Estadística y de la normativa citada en los considerandos de la presente resolución, el Gerente del Instituto Nacional de Estadística:





**RESUELVE**

- I. Aprobar la “**Política Institucional de Seguridad y uso de Tecnologías de la Información**” **Versión 2**, que establece lineamientos que orientan el uso adecuado, seguro y responsable de los sistemas, equipos y servicios informáticos institucionales, asegurando la protección de la información estadística y administrativa que se genera, procesa y resguarda en el INE.
- II. Se instruye al Director de Informática del Instituto Nacional de Estadística, para que proceda a socializar la incorporación de la política aprobada, a todo el personal y contratistas a su cargo, así como, velar por su debida implementación y aplicación.
- III. Pase a Planificación para que, por vía electrónica, socialice la “**Política Institucional de Seguridad y uso de Tecnologías de la Información**” **Versión 2**, a todas las Direcciones y Órganos de Apoyo Técnico.
- IV. La presente resolución surte efectos de manera inmediata.

**Notifíquese:** Subgerencia Administrativa Financiera, Subgerencia Técnica, Dirección Financiera, Dirección Administrativa, Dirección de Informática, Asesoría Jurídica y Auditoría Interna.

  
**Mgtr. Oscar José Chávez Valdez**  
Gerente







# **Instituto Nacional de Estadística**









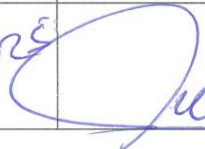

## **POLÍTICA INSTITUCIONAL DE SEGURIDAD Y USO DE TECNOLOGÍAS DE LA INFORMACIÓN**

**DIRECCIÓN DE INFORMÁTICA  
POL-DI-V02**

**VERSIÓN 02**

**GUATEMALA, DICIEMBRE 2025**

## Cuadro de Validación

Validación de la Política Institucional de Seguridad y Uso de Tecnologías de la Información, Versión 02			
Elaborado por	Cargo	Fecha	Firma
Ing. César Estuardo Oliva Marroquín	Jefe del Departamento de Análisis, Desarrollo y Mantenimiento de Sistemas	4/12/2025	
			
Revisado y Vo. Bo. por	Cargo	Fecha	Firma
Ing. Gandy Ricardo Tejada Castañeda	Director de Informática	4/12/2025	
			
Revisado por	Cargo	Fecha	Firma
Lic. Francisco Vallejo Bolaños	Coordinador de Organización Institucional	04/12/25	
			
Licda. Ana Verónica García Juárez	Directora de Planificación	04/12/2025	
			
Validado por	Cargo	Fecha	Firma
Lic. Edgar Daniel Ulbán Leiva	Subgerente Administrativo y Financiero	05/12/2025	
			

## Contenido

Introducción.....	1
Objetivos .....	2
Base Legal .....	3
Alcance .....	4
Incumplimiento .....	5
Principios.....	6
Política Institucional de Seguridad y Uso de Tecnologías de la Información .....	8
Responsables .....	8
Justificación .....	11
Definición .....	11
Estrategias .....	11
Glosario de Términos .....	19

## Introducción

El presente documento constituye un instrumento administrativo y normativo de observancia obligatoria para todo el personal de la Institución, incluyendo a los usuarios que, de forma directa o indirecta, hacen uso de los recursos informáticos y de comunicación que forman parte de la infraestructura tecnológica del INE.

Su propósito es establecer lineamientos claros que orienten el uso adecuado, seguro y responsable de los sistemas, equipos y servicios informáticos institucionales, asegurando la protección de la información estadística y administrativa que se genera, procesa y resguarda en la Institución. Su contenido busca garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad operativa de los servicios tecnológicos, contribuyendo al cumplimiento de los objetivos estratégicos del INE.

La Política está compuesta por un conjunto de normas y estrategias que definen la forma en que deben administrarse y protegerse los recursos informáticos institucionales, estableciendo responsabilidades, restricciones y mecanismos de control para prevenir riesgos, minimizar incidentes y asegurar el cumplimiento de los marcos legales y normativos aplicables.

La Dirección de Informática, en coordinación con las demás dependencias del INE, será la encargada de velar por la aplicación, seguimiento y actualización de las políticas aquí contenidas, asegurando que se mantengan alineadas con los avances tecnológicos, las necesidades institucionales y las exigencias de los organismos reguladores. Asimismo, todos los manuales y documentos técnicos elaborados por la Dirección deberán ajustarse y cumplir con las disposiciones establecidas en esta política, garantizando coherencia y uniformidad en la gestión tecnológica institucional.

El Instituto Nacional de Estadística reafirma su compromiso de fortalecer la seguridad de la información, proteger la infraestructura tecnológica institucional y garantizar la prestación de servicios informáticos confiables y eficientes que respalden la generación, análisis y difusión de estadísticas oficiales de calidad para el país, así como el cumplimiento de su obligación legal de resguardar y proteger la información estadística del Estado, asegurando su integridad, confidencialidad y disponibilidad para la toma de decisiones.

## Objetivos

### General:

Garantizar la seguridad de la información y la continuidad de los servicios informáticos mediante su buen uso, asegurando la confiabilidad, disponibilidad e integridad de los sistemas y de la información que resguardan. Asimismo, asegurar el apoyo a las operaciones del Instituto Nacional de Estadística, optimizando el uso de los recursos informáticos y de comunicación institucionales, contribuyendo al cumplimiento de la misión y objetivos estratégicos de la Institución.

### Específicos:

- Garantizar el uso responsable y apropiado de los recursos de Tecnologías de la Información y Comunicación (TIC) del INE, promoviendo la protección y seguridad de la información.
- Estandarizar e integrar los sistemas de información y las aplicaciones informáticas utilizadas para la gestión y procesamiento de datos estadísticos, asegurando su confiabilidad y compatibilidad.
- Reducir las interrupciones en la disponibilidad y funcionamiento de los servicios informáticos, previniendo daños o afectaciones por uso inapropiado, accidentes o acciones intencionales.
- Definir claramente las responsabilidades de los usuarios en el uso de los equipos, sistemas y servicios informáticos institucionales.
- Establecer restricciones y prohibiciones para el uso de los equipos y sistemas informáticos del INE, con el fin de proteger la información y los recursos tecnológicos de la Institución.

## Base Legal

- Constitución Política de la República de Guatemala;
- Ley Orgánica del Instituto Nacional de Estadística, Decreto Ley Número 3-85 y su Reglamento.
- Ley de Acceso a la Información Pública, Decreto Número 57-2008 del Congreso de la República de Guatemala.
- Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala.
- Ley de Contrataciones del Estado, Decreto Número 57-92 del Congreso de la República de Guatemala.
- Código Penal de Guatemala, Decreto 17-73 del Congreso de la República de Guatemala
- Ley de Prevención y Protección contra la Ciberdelincuencia, Decreto Número 39-2022 del Congreso de la República de Guatemala.
- Reglamento Orgánico Interno del Instituto Nacional de Estadística, Acuerdos de Gerencia Número 02-2019 y Número 03-2019.
- Manual de Auditoría de Tecnología de la Información, Acuerdo Número A-047-2021 de la Contraloría General de Cuentas.
- Normas Generales y Técnicas de Control Interno Gubernamental, Acuerdo Número A-039-2023 de la Contraloría General de Cuentas.

## Alcance

La presente Política es aplicable a todos los usuarios de los recursos informáticos del INE, incluyendo funcionarios, trabajadores y contratistas del Instituto Nacional de Estadística, ya sea de forma compartida o de uso individual, y que operen de manera aislada o interconectada a través de redes. En caso de presentarse un conflicto entre dos o más políticas, prevalecerá aquella que resulte más favorable para la protección y resguardo de los intereses legítimos de la Institución.

## Incumplimiento

La infracción a estas políticas podrá conllevar medidas conforme con la normativa aplicable, incluyendo la finalización de la relación laboral o contractual.

Son causas graves de acuerdo con esta Política las siguientes:

- Divulgación/distribución no autorizada de información institucional.
- Falsificación o robo de datos.
- Robo o daño intencional de equipos/recursos informáticos.
- Almacenamiento de información pornográfica, discriminatoria u ofensiva.
- Reincidencia en la infracción de normas.

## Principios

Los principios que rigen de manera general la gestión, uso y resguardo de los recursos informáticos y de la información en el Instituto Nacional de Estadística, son los siguientes:

1. Seguridad de la información: La información debe mantenerse completa, exacta y confiable, a través de controles y mecanismos de seguridad que prevengan su modificación, eliminación o alteración indebida, ya sea accidental o intencional.
2. Confidencialidad y resguardo de la información: Toda la información estadística y administrativa generada, recopilada y almacenada por el INE está protegida por la Ley Orgánica del Instituto Nacional de Estadística, Decreto Ley Número 3-85, la cual establece en el artículo 25 la obligación de resguardar la confidencialidad de los datos suministrados por personas naturales o jurídicas, por lo que para dar cumplimiento, la información será resguardada de acuerdo con su nivel de sensibilidad (pública, de uso interno, confidencial) de acuerdo con la Ley de Acceso a la Información Pública y otra normativa vigente garantizando la protección de la información y la confianza de la población.
3. Propiedad institucional: Toda la información generada, recopilada, y almacenada en los sistemas, equipos, actividades y servicios informáticos del INE es propiedad exclusiva de la Institución. Ningún usuario podrá utilizarla para fines personales, comerciales o ajenos a las funciones institucionales.
4. Disponibilidad del servicio: Los recursos informáticos deberán estar disponibles de manera oportuna para el cumplimiento de las funciones institucionales, planes de respaldo, contingencia y recuperación para asegurar esta continuidad.
5. Uso adecuado de los recursos: Toda persona deberá utilizar los equipos y servicios informáticos de manera responsable y conforme a la Política establecida, evitando cualquier práctica que pueda poner en riesgo la seguridad de la información o la operación de los servicios.
6. Responsabilidad individual: Cada usuario es responsable de la información y recursos a los que tenga acceso, debiendo cumplir con la Política establecida y reportar de inmediato cualquier incidente, irregularidad o amenaza que pueda comprometer la seguridad o continuidad de los servicios informáticos.
7. Transparencia: La gestión de los recursos informáticos y de la información debe ser transparente, asegurando que todos los procesos sean trazables y auditables, permitiendo la rendición de cuentas ante autoridades y organismos de control, fortaleciendo la confianza institucional y ciudadana.

# **POLÍTICA INSTITUCIONAL DE SEGURIDAD Y USO DE TECNOLOGÍAS DE LA INFORMACIÓN**

## Política Institucional de Seguridad y Uso de Tecnologías de la Información

### Responsables:

**Dirección de Informática:** Es responsable de la correcta aplicación, seguimiento y actualización de la Política Institucional de Seguridad y Uso de Tecnologías de la Información, velando porque las decisiones y procedimientos sobre recursos tecnológicos se apeguen a principios de seguridad, eficiencia, confiabilidad y a la normativa institucional y nacional vigente.

### Atribuciones y responsabilidades:

- **Seguridad de la información:** Es función de la Dirección de Informática definir el marco de seguridad y protección de datos de la institución, estableciendo controles mínimos y métricas de confiabilidad, disponibilidad e integridad de la información. La Dirección de Informática está facultada para monitorear, auditar y registrar el uso de los recursos tecnológicos institucionales (correo, navegación, historial de uso, archivos compartidos) cuando exista sospecha fundada de incumplimiento, incidente de seguridad o por requerimiento de auditorías internas/externas, garantizando siempre el apego a la normativa vigente.
- **Gobernanza y actualización normativa:** La Dirección de Informática es responsable de aplicar y mantener vigente la presente Política, junto con los lineamientos y estándares técnicos relacionados. Además, debe proponer mejoras y actualizaciones de acuerdo con la evolución tecnológica y las recomendaciones derivadas de auditorías internas o externas.
- **Gestión estratégica y priorización:** Corresponde a la Dirección de Informática el desarrollo de la tecnológica institucional y priorizar iniciativas de acuerdo con su impacto, los riesgos asociados, la necesidad de continuidad operativa y la disponibilidad de presupuesto y personal. Asimismo, debe evaluar e impulsar soluciones que mejoren la seguridad, el rendimiento y los costos, dando preferencia al software libre cuando sea técnica y económicamente viable.
- **Gestión de riesgos y continuidad:** La Dirección de Informática debe liderar el ciclo de gestión de riesgos en tecnologías de la información, incluyendo la implementación y actualización de los planes de continuidad (BCP) y recuperación ante desastres (DRP). También debe coordinar la realización de pruebas periódicas de continuidad con las áreas dueñas de procesos críticos.
- **Arquitectura y estandarización tecnológica:** La Dirección de Informática establece principios de arquitectura tecnológica, catálogos y listas blancas de servicios, softwares, entre otros, políticas de versiones y criterios de

obsolescencia. También debe asegurar la adecuada separación de ambientes y la trazabilidad de todos los cambios realizados en los sistemas.

- **Cumplimiento y auditoría:** La Dirección de Informática debe garantizar la alineación de los procesos informáticos con la Ley Orgánica del INE, las Normas de Control Interno Gubernamental y la normativa aplicable. Asimismo, debe coordinar la atención a auditorías y dar seguimiento a los planes de remediación que se deriven de ellas.
- **Gestión de acceso y segregación de funciones:** Le corresponde a la Dirección de Informática establecer criterios y modelos de roles y perfiles de usuario, implementar la segregación de funciones y realizar revisiones periódicas de accesos. También debe ordenar las altas, bajas o suspensiones de usuarios cuando corresponda, ya sea por vencimiento de contrato, mandato de autoridad o incidentes de seguridad.
- **Dirección del ciclo de desarrollo y datos:** La Dirección de Informática define las prácticas para el ciclo de vida del software, desde el levantamiento de requerimientos hasta las pruebas, liberaciones, documentación y mantenimiento. Asimismo, debe establecer lineamientos de gobierno de datos, garantizando la calidad, existencia de catálogos y responsables funcionales en cada área.
- **Relación con usuarios y soporte a procesos:** Es responsabilidad de la Dirección de Informática asegurar que los servicios tecnológicos respalden adecuadamente los procesos estadísticos y administrativos de la institución. Además, debe brindar apoyo oportuno, resolver problemas y coordinar acciones con las áreas dueñas de cada proceso.
- **Gestión presupuestaria y licenciamiento:** La Dirección de Informática debe conducir la planificación y ejecución presupuestaria en materia tecnológica, emitir dictámenes técnicos previos a adquisiciones y licenciamientos, y llevar un control actualizado de la matriz de licencias y contratos de software institucional.
- **Vinculación con terceros:** Le corresponde a la Dirección de Informática autorizar y supervisar la subcontratación de servicios tecnológicos y la recepción de donaciones de activos informáticos, garantizando siempre el cumplimiento de los estándares de seguridad y la inclusión de estas acciones en el Plan Operativo Anual.
- **Monitoreo y métricas (KPIs/KRIs):** La Dirección de Informática debe definir indicadores de desempeño y riesgo, tales como niveles de servicio, disponibilidad, número de incidentes, vulnerabilidades detectadas, copias de respaldo realizadas, tiempos de atención y cumplimiento de controles, informando periódicamente a la Gerencia y Subgerencias.

- **Formación y cultura de seguridad:** Es deber de la Dirección de Informática liderar programas de concientización y capacitación obligatoria para el personal en temas de seguridad informática (por ejemplo: phishing, contraseñas seguras, protección de datos, trabajo remoto). Asimismo, debe mantener canales de reporte abiertos y materiales de referencia accesibles a toda la institución.

**Usuarios en general:** Los usuarios de los recursos informáticos del Instituto Nacional de Estadística son responsables de utilizarlos de manera ética, segura y exclusivamente institucional. Toda acción realizada bajo sus credenciales personales o en recursos asignados será atribuida al titular, salvo casos excepcionales autorizados por la Dirección de Informática con visto bueno de la Subgerencia Administrativa y Financiera. El uso indebido, la omisión de deberes o el incumplimiento de esta Política y de la normativa aplicable podrá conllevar sanciones administrativas y legales.

Atribuciones y responsabilidades:

- **Cumplir la política:** El usuario debe acatar los principios, lineamientos y normas de esta Política y de la normativa institucional relacionada, aplicando en todo momento medidas de seguridad y confidencialidad sobre la información que administra o genera.
- **Custodia de credenciales y equipos:** Cada usuario debe bloquear sus sesiones y equipos al ausentarse, resguardar sus credenciales personales e intransferibles y utilizar de forma responsable los recursos tecnológicos que le han sido asignados.
- **Uso exclusivo institucional:** Los recursos informáticos y servicios tecnológicos se emplearán únicamente para fines laborales vinculados a la misión del INE; queda prohibido cualquier uso personal, comercial o ajeno a las funciones institucionales.
- **Conducta y contenido:** El uso de sistemas y redes debe ser respetuoso y profesional, evitando cualquier forma de acoso o uso indebido, así como, el acceso, descarga o almacenamiento de contenidos no relacionados con las tareas institucionales o contrarios a los valores del INE.
- **Confidencialidad de la información:** Está prohibido divulgar información institucional sin autorización expresa; toda manipulación de datos debe realizarse conforme a la Ley Orgánica del INE y a lo establecido en esta Política.
- **Reporte de incidentes:** Ante cualquier vulnerabilidad, anomalía o incidente de seguridad, el usuario deberá reportarlo de inmediato a la Dirección de Informática por los canales oficiales habilitados, para su atención y seguimiento.

- Responsabilidad sobre recursos temporales (029/Subgrupo 18): A personas contratadas por servicios técnicos o profesionales bajo el renglón presupuestario 029 y Subgrupo 18, se le podrán asignar recursos tecnológicos, incluyendo equipos y correos institucionales, únicamente para la ejecución de las actividades establecidas en su contrato. Esta asignación tiene fines estrictamente operativos y de seguridad, no implicando una relación laboral distinta a la contratación temporal vigente, con el fin de que se cumplan todas las políticas de seguridad y uso responsable establecidas por el INE en la realización de esas actividades y productos generados. Una vez finalizado el servicio, las cuentas serán desactivadas y los equipos deberán quedar en resguardo.

#### **Justificación:**

La Política Institucional de Seguridad y Uso de Tecnologías de la Información es fundamental para garantizar un entorno tecnológico seguro, eficiente y productivo para toda la institución, de forma clara, concisa, con el fin de estar disponibles para todos los usuarios responsables de la seguridad de la información, incluidos los usuarios de los sistemas de la Institución que intervengan en la protección de la información, quienes deben conocer y cumplir con las normas para evitar riesgos y garantizar la seguridad.

#### **Definición:**

La Política Institucional de Seguridad y Uso de Tecnologías de la Información es un conjunto de normas y directrices documentadas que definen la estrategia general para proteger los activos de información, estableciendo roles, responsabilidades, y los controles necesarios para mantener la confidencialidad, integridad y disponibilidad de los datos y sistemas de la Institución.

#### **Estrategias:**

Las estrategias son acciones que definen como la institución utilizará la tecnología de la información para apoyar y alcanzar los objetivos y metas, a través de la regulación, el resguardo, uso y administración de los recursos tecnológicos, garantizan la exclusividad de uso institucional, la seguridad de la información y la continuidad operativa. Estas son de cumplimiento obligatorio para todos los usuarios:

#### **Seguridad de la información:**

- Prohibición de BitLocker: No está permitido habilitar la función de BitLocker en los discos duros institucionales, lo que interfiere con los esquemas centralizados de administración y respaldo.

- **Conexión de equipos externos:** Los dispositivos externos no autorizados no pueden conectarse a la red institucional. En casos excepcionales, deberán contar con antivirus actualizado y cumplir con las condiciones técnicas que determine la Dirección de Informática.
- **Integridad de la red interna:** Se prohíbe reproducir contenido no laboral dentro de la red institucional, alterar configuraciones sin autorización, usurpar equipos, vulnerar mecanismos de seguridad, ejecutar ataques de denegación de servicio (DoS) o intentar evadir los controles establecidos.
- **Supervisión de la Dirección de Informática:** La Dirección de Informática debe mantener un monitoreo constante de la red, actualizar periódicamente los filtros de acceso y garantizar la vigencia de los planes de continuidad y recuperación (BCP/DRP).

### Equipos y servicios de tecnologías de la información:

- **Uso exclusivo institucional:** El equipo informático, el software instalado, el acceso a internet, el correo institucional, las licencias y demás servicios tecnológicos son de uso exclusivo para fines institucionales. Se prohíbe expresamente su utilización para actividades personales, comerciales o ajenas a la misión del INE.
- **Acceso con credenciales personales:** Todo acceso a recursos tecnológicos debe realizarse mediante un usuario y contraseña personales, que son intransferibles. El titular es plenamente responsable de su uso, resguardo y de las acciones realizadas bajo dichas credenciales.
- **Puertos USB:** Los puertos USB de los equipos institucionales permanecen bloqueados por defecto. Su habilitación requiere una solicitud justificada y autorización de la Dirección de Informática, con visto bueno de la Subgerencia Administrativa y Financiera. Quien reciba autorización debe garantizar el uso seguro del dispositivo y prevenir la fuga de información o la introducción de software malicioso.
- **Buenas prácticas de uso físico:** Queda prohibido conectar equipos no informáticos a los UPS, consumir alimentos o bebidas cerca de los equipos, mantenerlos encendidos de forma innecesaria o manipular hardware, software o etiquetas de seguridad sin la autorización correspondiente.

### Correo electrónico institucional:

- El correo institucional es de uso exclusivo laboral; Queda prohibido emplear cuentas personales para fines institucionales o vulnerar cuentas existentes.
- Los usuarios deben marcar como spam y reportar de inmediato al correo [ayudait@ine.gob.gt](mailto:ayudait@ine.gob.gt) cualquier mensaje sospechoso.

- Las cuentas son personales e intransferibles, y su creación solo procede mediante solicitud del jefe inmediato a la Dirección de Informática.
- Las cuentas inactivas por más de 90 días serán deshabilitadas automáticamente. En caso necesario, la Dirección de Informática podrá reactivarlas dentro de un plazo de 20 días calendario posteriores a su desactivación.
- Prohibición de compartir listados de correos institucionales sin autorización expresa.
- Todo contenido enviado debe ser acorde a los valores institucionales. Cuando corresponda, el usuario debe resguardar externamente los archivos adjuntos importantes.
- Al egreso de un usuario, el Departamento de Recursos Humanos deberá solicitar formalmente a la Dirección de Informática la deshabilitación de la cuenta institucional.

### Internet y WiFi:

- Prohibición de acceder a sitios no relacionados con actividades institucionales o que sean contrarios a los valores del INE, tales como pornografía, juegos, redes sociales, servicios de streaming, entre otros.
- No se permite la descarga de contenido no autorizado ni el intercambio de información confidencial a través de internet.
- Queda prohibido todo tipo de acoso o conducta intimidatoria en línea.
- Exclusividad de uso de la red WiFi institucional; Los dispositivos personales no están autorizados, salvo casos excepcionales con autorización expresa.
- Para acceder de forma temporal a sitios restringidos (como redes sociales, contenido multimedia o páginas de compras y cotizaciones) se debe presentar un oficio a la Dirección de Informática con visto bueno de la Subgerencia Administrativa y Financiera, indicando sitios y periodo requerido.

### Accesos, contraseñas y Active Directory (AD):

- Cambio de contraseñas cada 90 días, con un mínimo de ocho caracteres y al menos tres tipos distintos (mayúsculas, minúsculas, números y símbolos). No se permite reutilizar las tres últimas, incluir datos personales ni usar la opción "Recordar contraseña" en navegadores.
- El sistema bloqueará la cuenta tras cinco intentos fallidos de acceso y notificará la caducidad de la contraseña con tres días de anticipación.

- Cada usuario debe contar con una cuenta única en Active Directory, no estando permitidas cuentas genéricas o compartidas, y todas deben pertenecer al dominio institucional.
- Los permisos se asignarán bajo el principio de mínimo privilegio, de acuerdo con el rol del usuario (administrador, estándar, técnico). La Dirección de Informática es responsable de organizar los grupos de seguridad, mantener redundancia y replicación en los controladores de dominio, y configurar los permisos de acceso a carpetas y archivos compartidos.

#### Bases de datos:

- La Dirección de Informática es responsable de administrar las bases de datos institucionales, priorizando el uso de motores de software libre siempre que sea técnica y económicamente viable.
- Las áreas usuarias son responsables de la calidad de la información que ingresan y deben comunicar de manera oficial a la Dirección de Informática las validaciones que se requieran y los responsables funcionales de cada desarrollo.
- Los accesos se otorgan por defecto en modo de consulta y cualquier cambio en la estructura de las bases de datos, debe solicitarse formalmente para su evaluación y aprobación por la Dirección de Informática.
- La Dirección de Informática debe garantizar la disponibilidad, seguridad e integridad de las bases de datos, asegurar la separación de entornos de desarrollo y producción, aplicar esquemas de respaldo periódicos, velar por la continuidad operativa de los sistemas que las utilizan y resguardo de la información.

#### Backups:

- Los respaldos deben realizarse únicamente sobre archivos de carácter institucional, quedando prohibido almacenar o proteger información personal en los equipos institucionales.
- Los usuarios que cuenten con licenciamiento en la nube están obligados a sincronizar sus archivos para garantizar su disponibilidad y continuidad de trabajo.
- La Dirección de Informática es responsable de realizar y mantener los respaldos de la información contenida en los equipos asignados a los usuarios, asegurando la continuidad y protección de los datos institucionales.

- Todos los respaldos se almacenarán en el servidor institucional de copias de seguridad, bajo la administración de la Dirección de Informática, el acceso estará restringido exclusivamente al personal autorizado.
- La Dirección de Informática, a través del Departamento de Infraestructura, debe mantener un inventario actualizado de respaldos, así como, de configurar, monitorear y verificar periódicamente su correcta ejecución. Además, realizará una conciliación semestral entre el inventario y la herramienta de almacenamiento.
- Los directores o jefes que requieran la consulta de un respaldo deberán gestionarlo mediante oficio dirigido a la Dirección de Informática, justificando la necesidad del acceso.

### Trabajo remoto:

- En el caso de autorización para trabajo remoto de un usuario por parte de las autoridades competentes, si es necesario, podrá conectar a la red institucional únicamente por medio de Escritorio Remoto de Windows a través de VPN.
- Las solicitudes de acceso remoto deberán gestionarse mediante oficio por parte de la dirección correspondiente, con el visto bueno de su director, para su atención por la Dirección de Informática.
- La Dirección de Informática es responsable de configurar las conexiones VPN, validar que se empleen protocolos seguros y garantizar que no se instale software de acceso remoto no autorizado en equipos de colaboradores no autorizados.
- En los casos en que se habilite el acceso desde dispositivos no institucionales, la Dirección de Informática emitirá los lineamientos técnicos necesarios y verificará su cumplimiento.
- La confidencialidad, integridad y uso adecuado de la información procesada durante el teletrabajo son responsabilidad directa del usuario que accede a los sistemas.

### Portal web institucional:

- Toda publicación, alta o baja de contenido en el portal web institucional debe contar con la autorización de la dirección responsable y el visto bueno de la Gerencia. Cada dirección es responsable del contenido que publica.
- La Dirección de Informática debe garantizar que el portal web institucional permanezca activo y disponible las 24 horas del día, los 7 días de la semana.

- Los usuarios con acceso al sistema de publicaciones son responsables de resguardar sus credenciales y utilizarlas de manera segura.

Software (adquisición, licenciamiento e instalación):

- Toda adquisición de software o servicios informáticos debe contar con un dictamen técnico previo de la Dirección de Informática, que asegure los estándares de seguridad y la arquitectura tecnológica vigente.
- Solo se permite el uso de software autorizado, estandarizado y con licenciamiento válido; queda prohibida la instalación o utilización de aplicaciones no autorizadas.
- El control centralizado de licencias corresponde a la Dirección de Informática, incluyendo las asociadas a servidores, telecomunicaciones, seguridad informática y software institucional.
- Las direcciones pueden financiar la adquisición de licencias especializadas con su propio presupuesto o con el de la Dirección de Informática.

Desarrollo de software:

- Toda solicitud de desarrollo de software debe realizarse mediante oficio formal, que incluya la justificación de la necesidad, el objetivo del sistema, su alcance, los usuarios y procesos involucrados, los datos a manejar y el tiempo estimado de implementación.
- La unidad solicitante debe designar un enlace técnico-funcional, participar activamente en reuniones, validaciones y entregar de manera completa y oportuna todos los insumos necesarios para el desarrollo.
- El proceso comprende las fases de levantamiento y análisis de requerimientos, así como, diseño de la solución, construcción, programación, pruebas, validaciones, aprobación final por parte del solicitante, implementación y mantenimiento. La Dirección de Informática definirá los detalles técnicos, metodológicos y de control en cada fase.
- La Dirección de Informática, a través del Departamento de Desarrollo, es responsable de recibir, evaluar y priorizar las solicitudes con base en su criticidad, impacto institucional, disponibilidad de recursos y alineación estratégica. Además, gestiona el ciclo de vida del desarrollo de software, que asegure la documentación adecuada, la separación de ambientes de desarrollo, pruebas y producción, así como trazabilidad y calidad de los entregables.

- En caso de incumplimiento por parte del solicitante (falta de oficio, ausencia de enlace designado, no participación en reuniones, no entrega de insumos o cambios frecuentes sin justificación), la Dirección de Informática podrá suspender o no iniciar el desarrollo solicitado. La reactivación del proyecto quedará sujeta a la subsanación de los incumplimientos y a la disponibilidad técnica en ese momento.
- Todo desarrollo de software, scripts, bases de datos, informes, metodologías, documentación técnica y cualquier otro entregable generado por usuarios en el marco de sus funciones institucionales es propiedad exclusiva del INE.
- La custodia, administración y control de versiones de dichos desarrollos quedará bajo la responsabilidad de la Dirección de Informática, quien garantizará su trazabilidad y resguardo en repositorios institucionales autorizados.
- La identificación de los usuarios en los nuevos sistemas, a partir de la entrada en vigencia de la presente Política, se realizará mediante Active Directory. Todos los sistemas que se desarrollen o implementen posteriormente deberán validar la información de los usuarios a través de esta herramienta. En el caso de los sistemas existentes previo a la aplicación de esta Política, la Dirección de Informática será la responsable de registrar y administrar la información de los usuarios directamente en las bases de datos correspondientes.

### Gestión de activos:

- La baja de activos informáticos se realizará de acuerdo con la normativa vigente, el personal de soporte técnico realizará previamente el respaldo o borrado seguro de la información según corresponda.
- Los usuarios tienen prohibido remover o agregar componentes de hardware o software, así como, extraer recursos informáticos; en caso de tener que modificar componentes de los recursos institucionales, se hará de acuerdo con la normativa vigente.
- Todo activo donado a la Institución debe tramitarse siguiendo el proceso administrativo correspondiente en las direcciones responsables.

### Manejo y actualización de políticas:

- Todos los usuarios están obligados a conocer y cumplir las políticas informáticas institucionales vigentes.
- La Dirección de Informática es responsable de velar por su cumplimiento, orientar y aclarar dudas, así como, coordinar que los técnicos regionales visiten y monitoreen las Delegaciones Departamentales, reportando las anomalías al Coordinador Regional correspondiente.

- La Dirección de Informática debe mantener la Política actualizadas de acuerdo con la evolución tecnológica y los procesos de modernización institucional.
- La Dirección de Informática informará al Departamento de Recursos Humanos sobre cualquier incumplimiento de la Política, con el fin de que se tomen las acciones pertinentes conforme a la normativa institucional.

## Glosario de Términos

<b>BitLocker:</b>	Es una función de seguridad de Windows que cifra los datos de las unidades de disco para proteger la información confidencial. Su objetivo es prevenir el acceso no autorizado a la información en caso de que el dispositivo sea perdido, robado o si el disco duro es extraído.
<b>Correo electrónico:</b>	Redacción, envío o recepción de mensajes sobre sistemas de correo.
<b>Correo no solicitado:</b>	Correo electrónico en el cual no existe relación previa entre las partes y el destinatario no ha consentido explícitamente en recibir la comunicación.
<b>Correo Spam:</b>	Correo electrónico sin consentimiento o aprobación del destinatario, generalmente en forma masiva y con fines comerciales en el cual no existe relación previa entre las partes y el destinatario específico.
<b>Cortafuegos (firewall):</b>	Un sistema (hardware, software o una combinación de los dos), que se instala entre una red privada o una red pública para impedir accesos no autorizados, hacia o desde la red privada.
<b>Datos:</b>	Presentación de hechos, conceptos o instrucciones en una manera, apropiada para comunicación interpretación o procesamiento manual o automático.
<b>Datos personales:</b>	Información que identifica o describe a un individuo.
<b>Información:</b>	Es el significado asignado a los datos por medio de convenciones aplicadas a ellos.
<b>Integridad:</b>	Características de los datos y la información de ser y permanecer exactos y completos.
<b>Riesgo:</b>	Es una pérdida o daño futuro potencial que puede surgir por alguna acción presente.
<b>Seguridad:</b>	Medidas tomadas para reducir el riesgo de: 1) Acceso y uso no autorizado; y, 2) Daño o pérdida de los recursos, por algún desastre, error humano o fallo en los sistemas por una acción maliciosa.

**VPN:** Red Privada Virtual, es un servicio que crea una conexión segura y cifrada entre un dispositivo y el internet, permitiendo navegar de forma privada y segura.