NORMATIVO PARA LA ADMINISTRACIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA DE RED DEL INDE Y SUS COMPONENTES

División de Desarrollo Informático

Guatemala, agosto de 2021

NORMATIVO PARA LA ADMINISTRACIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA DE RED DEL INDE Y SUS COMPONENTES

ÍNDICE

ÍNDICE

ACUERDO No. GG-A-30-2021

CONSIDERANDO:

Que el Decreto Número 64-94 del Congreso de la República de Guatemala y sus Reformas, Ley Orgánica del Instituto Nacional de Electrificación -INDE-, establece que el mismo, es una entidad estatal, autónoma y descentralizada, que goza de autonomía funcional, patrimonio propio, personalidad jurídica y plena capacidad para adquirir derechos y contraer obligaciones en materia de su competencia. El cual se rige por su Ley Orgánica, disposiciones legales aplicables, reglamentos internos y acuerdos que emita el Consejo Directivo.

CONSIDERANDO:

Que es necesario elaborar instrumentos administrativos que permitan el ordenamiento, la estandarización, administración y seguridad de los componentes y equipos de conexión en la Red Institucional, facilitando contar con una Infraestructura confiable y segura para el acceso de los diferentes usuarios a los servicios informáticos.

POR TANTO:

La Gerencia General en el uso de las facultades que le confieren los Artículos 17 y 18 del Decreto 64-94 del Congreso de la República de Guatemala y sus Reformas, Ley Orgánica del Instituto Nacional de Electrificación INDE,

ACUERDA:

Aprobar el siguiente:

NORMATIVO PARA LA ADMINISTRACIÓN Y SEGURIDAD DE LA INFRAESTRUCTURA DE RED DEL INDE Y SUS COMPONENTES

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto y Ámbito de Aplicación. Establecer las normas adecuadas para la administración de hardware y software que conforman la Infraestructura de Red Institucional, manteniendo un orden desde su implementación, control y seguridad en sus accesos tanto internos (Intranet) como externos (Internet) haciendo los sistemas informáticos confiables. Así como el uso y aplicación para todos los trabajadores de la Institución y usuarios externos que tengan acceso a los servicios informáticos o a los sistemas de información, así como a todos los equipos de computación que pertenezcan y formen parte de los activos fijos de la Institución.

Artículo 2. Administración, Seguridad y Control. La administración, seguridad y control del hardware, software y los componentes de la Infraestructura de Red Institucional, así como las conexiones por medio de enlaces y la telefonía IP hacia las diferentes sedes de la Institución, deben quedar centralizadas en la División de Desarrollo Informático.

Artículo 3. Definiciones. Para los efectos del presente normativo, se establecen las siguientes definiciones:

a) **Autenticar:** Proceso para verificar si el usuario o equipo es el auténtico y que cumpla con las credenciales que lo fundamenten.

b) **Cliente Liviano (Thin Client)**: Es un dispositivo cliente con sistema operativo dedicado a infraestructura cliente-servidor que depende primariamente del servidor central para las tareas de procesamiento.

c) **Conectividad**: Es la capacidad de un dispositivo de poder ser conectado, generalmente a un ordenador personal u otro dispositivo electrónico.

d) **Confidencialidad**: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

e) **Correo Electrónico:** Es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica.

f) **Criptografía:** Método que se basa en algoritmos matemáticos que persiguen cifrar el contenido de un mensaje. Por medio del cifrado, los datos legibles se convierten en ilegibles, por lo que, en consecuencia, únicamente podría accederse a los mismos mediante la clave precisa para descifrarlos. Entre las modalidades de cifrado se tiene la criptografía de clave simétrica y la criptografía de clave asimétrica.

g) **Diagnostico:** Consiste en comprobar el funcionamiento correcto de la mayoría de los componentes críticos del sistema, por medio de una serie de pruebas de bajo nivel sobre cada uno de los componentes y generar un informe con el resultado de todas las pruebas efectuadas.

h) **DDI:** División de Desarrollo Informático.

i) **Dirección IP:** Es un conjunto de número que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo.

j) **Disponibilidad**: Es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.

k) **Dominio:** Es una agrupación lógica de equipos y usuarios.

l) **Enlaces de Telecomunicaciones:** Es toda transmisión y recepción de señales de cualquier naturaleza, típicamente electromagnéticas, que contengan signos, sonidos imágenes o, en definitiva, cualquier tipo de información que se desee comunicar a cierta distancia.

m) **Equipo Activo**: Equipo que se encarga de distribuir en forma activa la información a través de la red, como conmutadores y enrutadores.

n) **Firewall:** Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar y descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

o) **Firma Electrónica:** Datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante con relación a la comunicación electrónica e identificar que el firmante aprueba la información recogida en la comunicación electrónica.

p) **Firma Electrónica Avanzada:** Es un medio criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. La legislación guatemalteca establece los siguientes requisitos para la firma electrónica avanzada: vinculación única con el firmante; debe permitir la

identificación de firmante; debe ser creada bajo medios que el firmante tenga bajo su exclusivo control.

q) **Firmware:** Es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

r) **Hardware:** Conjunto de los componentes que integran la parte material de una computadora, ordenador o un sistema informático.

s) **Infraestructura de Red**: Estructura de medio de transporte de datos, la cual debe cumplir estándares internacionales para proporcionar un nivel alto de confiabilidad.

t) **Internet:** Es un sistema de redes informáticas interconectadas mediante distintos medios de conexión, que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a plataformas digitales.

u) **Intranet:** Red entre computadoras montada para el uso exclusivo dentro de una empresa.

v) **Malware (Código Malicioso)**: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

w) **Obsolescencia:** Es la condición o estado en que se encuentra un producto que ya ha cumplido con una vigencia o tiempo programado para que siga funcionando.

x) **Red (Network):** Grupo de dispositivos de cómputo interconectados entre sí por un medio para propósitos de comunicación, independiente de su localización física y que comparten recursos.

y) **Red Privada Virtual:** VPN por sus siglas en inglés. Sesión de red protegida establecida a través de canales no protegidos (p.e. Internet). Se materializa en dispositivos en el perímetro para establecer sesiones cifradas.

z) **Sala de Equipos de Alimentación Ininterrumpida (UPS en siglas en inglés):** Es el área donde se resguardan dispositivos que, gracias a sus baterías y otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados. Sala de UPS en adelante.

aa) **Servidor:** Un dispositivo de red que ofrece servicios a varias computadoras.

ab) **Sistema por Nombres de Dominio:** DNS por sus siglas en inglés. Es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes como Internet o Intranet.

ac) **Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora, ordenador o un sistema informático.

ad) **Subcentro de Conectividad:** Es el área exclusiva dentro de un edificio para albergar los equipos de la red local de interconexión entre cada uno de los subsistemas del cableado estructurado.

ae) **Subdominio:** Es un subgrupo o subclasificación del nombre de dominio el cual es definido con fines administrativos u organizativos, que podría considerarse como un dominio de segundo nivel. Normalmente es una serie de caracteres o palabra que se escriben antes del dominio.

af) **Usuario Externo:** Todas las personas que no teniendo relación laboral con la Institución y que sean autorizados expresamente, a acceder de manera

temporal a los servicios que presta la División de Desarrollo Informático y/o utilizar los recursos informáticos propiedad del INDE.

ag) Usuario: Trabajador que utiliza una computadora personal (estación de trabajo) y los recursos informáticos que proporciona la División de Desarrollo Informático, como una herramienta para resolver de forma eficaz y eficiente sus funciones.

ah) Vida Útil: El tiempo en el cual la Institución espera obtener beneficios de productividad o económicos derivados de dicho equipo de cómputo ya que después de ese tiempo, los proveedores y/o fabricantes no pueden dar soporte técnico por garantía y desabastecimiento de piezas importantes para su funcionamiento.

Artículo 4. Uso de Red Institucional. Las siguientes disposiciones deben ser de cumplimiento general para todos los usuarios tanto de la Red Institucional como de los diferentes sistemas informáticos:

a) Velar por los recursos informáticos y de servicios de la red del INDE.

b) Bajo ninguna circunstancia se deben utilizar los recursos informáticos para realizar actividades prohibidas por las normas establecidas o por leyes nacionales o internacionales.

c) El equipo de computación convencional o un cliente liviano, proporcionado a cada usuario debe ser utilizado exclusivamente para todo lo relacionado con la gestión de sus funciones.

d) Las cuentas de usuario de red, de sistema auxiliar o de cualquier otro sistema que permita acceder con usuario y clave y que se brinden por medio de la División de Desarrollo Informático, son personales e intransferibles y queda bajo su responsabilidad el uso de las mismas.

e) La División de Desarrollo Informático puede solicitar en el momento de una auditoria de sistema la información necesaria para el registro de los datos de los diferentes usuarios, dicha información se debe manejar como sensible, por lo que se debe proveer el Formulario de Confidencialidad respectivo, el cual debe ser aceptado por parte del solicitante. Dicha información debe quedar bajo resguardo, y no podrá ser utilizada para ningún otro fin más que el dispuesto por la División de Desarrollo Informático o las autoridades del INDE.

f) La División de Desarrollo Informático debe propiciar la implementación y uso de firma electrónica o firma electrónica avanzada en los procesos que se consideren necesarios, como un método de autenticación y validación de la información por parte de los usuarios, estableciendo un nivel de seguridad.

g) Los usuarios que cuenten con autorización para el uso de computadoras personales convencionales o Cliente Liviano deben periódicamente realizar respaldos (backups) de la información Institucional que se maneje para el desarrollo de sus funciones.

h) Todos los usuarios deben atender los mensajes que la División de Desarrollo Informático envíe y ponerlos en práctica. No atenderlos puede ocasionar efectos negativos para las operaciones Institucionales.

i) Corresponde al personal técnico de la División de Desarrollo Informático la instalación de software y la evaluación del hardware, para su mantenimiento predictivo, preventivo y/o correctivo.

j) Los usuarios deben reportar al Departamento de Soporte Técnico, por medio de la línea y correo habilitados, las fallas de cualquier índole informática.

k) Las licencias de acceso al sistema auxiliar, ya sean de consulta u operativas, los cambios o ampliaciones de perfiles y accesos temporales, deben ser canalizados por la División de Desarrollo Informático.

l) La creación de nuevos usuarios del sistema auxiliar, los cambios y/o ampliaciones de perfiles, serán ejecutados por la División de Desarrollo Informático.

m) La inhabilitación de los usuarios tanto de red como de los diferentes sistemas informáticos, deben ser realizados con la notificación de baja definitiva por parte de la División de Recursos Humanos, exceptuando el personal contratado en los renglones 029 y 031 los cuales, al momento de crear la cuenta de usuario, la misma tendrá la vigencia establecida en el contrato o acuerdo de nombramiento.

n) El dominio Institucional **inde.gob.gt** y subdominios tanto de Internet como Intranet deben ser administrados por la División de Desarrollo Informático.

o) Los movimientos de la telefonía análoga en lo concerniente a lo físico son responsabilidad de la División de Servicios Administrativos y la parte lógica es responsabilidad de la División de Desarrollo Informático.

p) La telefonía digital IP, debe ser administrada en cuanto a las altas, bajas y cambios por la División de Desarrollo Informático.

q) Las conexiones por medio de enlaces de comunicación de datos, hacia los diferentes centros de trabajo de la Institución, deben ser administrados por la División de Desarrollo Informático.

CAPÍTULO II
ADMINISTRACIÓN Y SEGURIDAD

Artículo 5. Uso Seguro de la Infraestructura de Red. La utilización de la Infraestructura de Red Institucional se debe regir de acuerdo con las disposiciones siguientes:

a) El Departamento de Infraestructura y Telecomunicaciones de la División de Desarrollo Informático es el único órgano autorizado para coordinar la instalación, configuración y dar mantenimiento a la Infraestructura de conectividad a la Red de la Institución en todas sus modalidades.

b) Solo el personal del Departamento de Soporte Técnico, será el encargado de destapar, desarmar y manipular con fines de mantenimiento preventivo o correctivo los equipos informáticos propiedad del INDE.

c) Cada uno de los trabajadores del Departamento de Soporte Técnico debe tener una cuenta con permisos que le permitan únicamente realizar un adecuado soporte, otorgándole al usuario una cuenta limitada. Se exceptúa a los usuarios que debido a la naturaleza de sus funciones necesiten otro tipo de permisos, mismos que deben ser solicitados y debidamente fundamentados a la División de Desarrollo Informático.

d) El Usuario Externo que por necesidad Institucional comprobada deba conectar su equipo a la red, debe solicitar la configuración del mismo al Departamento de Soporte Técnico, para que inspeccione el equipo, con el fin de comprobar que no constituye un riesgo para la seguridad de los servicios, red y recursos informáticos de la Institución, además de evaluar la necesidad de conexión a la red y gestionar el direccionamiento provisto por el Departamento de Infraestructura y Telecomunicaciones.

e) Para toda computadora, sea de reciente asignación o no, se debe solicitar al Departamento de Soporte Técnico la instalación, configuración y su registro en el inventario de cómputo de la División de Desarrollo Informático.

f) La División de Desarrollo Informático, por medio del Departamento de Infraestructura y Telecomunicaciones, tiene la facultad de auditar el volumen de tráfico de la red para poder analizar el comportamiento y prevenir tráfico indeseable que puede ser causado por virus, instalaciones defectuosas o equipos de red dañados, con el fin de tomar las acciones preventivas y correctivas necesarias.

g) El usuario es el único responsable del mal uso que se le dé a los diferentes sistemas y dispositivos informáticos, a la Infraestructura, a la información (contenidos, comunicación, descargas, mantenimiento, veracidad, envío y recepción de información y ejecución de programas no autorizados), así como de cualquier tipo de dispositivo de almacenamiento interno o externo que utilice.

Los usuarios deben:

i. Usar los servicios de comunicación sólo para enviar y recibir mensajes e información propios y exclusivos de sus funciones.
ii. Realizar una verificación de la veracidad de la información que ingresa, envía o almacena en la red y/o los equipos de cómputo.
iii. Mantener en la carpeta "Mis Documentos" toda información relacionada con sus funciones, la cual de acuerdo al Procedimiento de Respaldo de la Información es la utilizada para realizar el resguardo de la información.

h) El usuario es responsable de ingresar a la web sólo a sitios seguros con respecto a contenido publicado en Internet, archivos descargados, programas ejecutados desde Internet, mensajes recibidos y demás información que pueda estar en Internet.

i) Asignación de direcciones de red (IP): La División de Desarrollo Informático, por medio del Departamento de Infraestructura y Telecomunicaciones es responsable de asignar y controlar el uso local de direcciones de red (IP) necesarias en la Infraestructura Institucional, para asegurar la integridad en el funcionamiento de la misma y evitar errores en la transmisión de los diferentes servicios informáticos que se utilizan.

j) Asignación de nombres: El Departamento de Soporte Técnico es el único órgano autorizado de gestionar el uso y asignación de nombres a los equipos de cómputo y estaciones de trabajo, también de asociarlos al dominio de red Institucional con la finalidad de mantenerlos identificados.

k) Todas las computadoras de la Institución deben ser configuradas exclusivamente por el Departamento de Soporte Técnico de la División, identificándolas con un nombre compuesto con la nomenclatura propia de la División de Desarrollo Informático y el nombre del usuario del equipo, permitiendo fácilmente conocer su ubicación además del usuario responsable. Debe asociarlas al dominio de Red Institucional y dotarlas de conectividad.

l) La creación de usuarios de la Red Institucional (dominio), se debe requerir a la División de Desarrollo Informático, adjuntando para el efecto, copia del Acuerdo de Gerencia General o del contrato del empleado.

m) Asignación de contraseñas: Las contraseñas a implementarse en el usuario de red o dominio (ingreso al equipo), deben seguir la regla 6-3, la cual debido a la interoperabilidad de los sistemas es la misma empleada en la autenticación del servicio de correo electrónico Institucional. La contraseña debe tener una longitud mínima de 6 caracteres con 3 variaciones: se obliga la utilización de por lo menos una (1) letra minúscula, una (1) letra mayúscula y un (1) número.

n) Información en red: El Departamento de Infraestructura y Telecomunicaciones debe mantener, planear e implementar el crecimiento de la Red Institucional para garantizar su funcionamiento óptimo y permanente.

o) La División de Desarrollo Informático puede suspender de forma total o parcial los servicios a los usuarios bajo causas plenamente justificadas y documentadas, dando aviso del mal uso, abuso o cualquier situación anómala que afecte los servicios tecnológicos de la Institución, dicho aviso debe darse a la autoridad correspondiente para la consecuente aplicación de las medidas disciplinarias establecidas en el Pacto de Condiciones de Trabajo INDE-STINDE.

p) La suspensión de conexión de la red, inhabilitación de servicio o alguna otra medida temporal se debe realizar por parte del personal de la División de Desarrollo Informático. Únicamente cuando un equipo de cómputo, equipo de conectividad o cualquier otro elemento de la Red Institucional presente riesgo para el desempeño de la misma o para los demás usuarios y debe ser notificado de manera verbal o por escrito según la naturaleza del riesgo.

q) La Unidad que requiera para su equipo de cómputo mantenimiento preventivo, compra de repuestos, accesorios y reparaciones, deberá solicitar el diagnóstico correspondiente elaborado por el Departamento de Soporte Técnico. La Unidad solicitante, será la responsable del pago y trámite administrativo que se requiera para ello.

r) Para la compra de equipo de cómputo nuevo a nivel Institucional, será la División de Desarrollo Informático la encargada de establecer las configuraciones mínimas necesarias de acuerdo a las necesidades de cada una de las unidades interesadas. La Unidad solicitante, será la responsable del pago y trámite administrativo que se requiera para ello.

Artículo 6. Seguridad de los Subcentros de Conectividad y Salas de UPS. Para mantener la seguridad de los subcentros de conectividad y salas de UPS se debe cumplir con lo siguiente:

a) Los Subcentros de Conectividad y Salas de UPS no podrán ser utilizadas como bodegas de material inflamable (cartón, papel, etc.) o cualquier otro material o equipo que obstaculice el flujo libre de aire en el mismo y sobre todo el acceso a los equipos en caso de emergencia o falla de los mismos.

b) En las áreas provistas para el alojamiento de los equipos, únicamente se permite la permanencia de personal de la División de Desarrollo Informático. En caso de excepciones se debe hacer solicitud de manera oficial escrita a la División de Desarrollo Informático.

c) En los centros de trabajo del interior de la República en los cuales no se cuente con un área para el alojamiento de los equipos de conexión, estos deben estar como mínimo dentro de un gabinete de seguridad con las condiciones de flujo de aire y seguridad, provistos de una llave, el Departamento de Infraestructura y Telecomunicaciones de la División de Desarrollo Informático debe contar con copia.

d) Todos los equipos de conectividad (activos) deben contar con un sistema de protección de energía eléctrica.

e) Cuando los equipos de conectividad y UPS estén en el centro de datos estos deben contar con todos los niveles y parámetros de seguridad establecidos para cada equipo.

Artículo 7. Administración y Gestión de los Equipos Activos. La División de Desarrollo Informático, por medio del Departamento de Infraestructura y Telecomunicaciones debe implementar en los equipos que lo permitan los siguientes controles de seguridad para el acceso, la autenticación y administración de los mismos:

a) Habilitar el cifrado de las contraseñas que se observan en los archivos de arranque de los equipos.

b) Habilitar la autenticación en la consola.

c) Habilitar la administración vía SNMPv2 o SNMPv3 de ser necesario.

d) Configurar en los equipos métodos de autenticación seguros, para administración vía web HTTPS, para administración por emulación de terminal SSHv2 o superior.

e) Crear una Lista de Control de Acceso (ACL) que permita el ingreso únicamente desde el segmento de red correspondiente.

f) Inhabilitar la opción de conexión por HTTP y acceder de modo terminal (Telnet).

g) Inhabilitar la administración vía SNMPv1.

h) Monitorear la red con el fin de identificar si los usuarios están corriendo herramientas de jaqueo (hack) o analizar paquetes de tránsito (sniffing).

i) Monitorear la red para verificar si los usuarios hacen buen uso del recurso de red, siempre teniendo en cuenta que la Red de la Institución se debe utilizar con fines de investigación o administrativos orientados al funcionamiento de la misma.

La actividad de monitorear depende de herramientas y equipos especializados para tal fin, en caso de no contar con los mismos, únicamente se ejecutarían muestras mediante la utilización de sniffer en los sitios que presenten fallas de red recurrentes.

j) Se debe contar con un servicio de mantenimiento de los diferentes equipos activos que incluya limpieza del hardware y la actualización periódica del firmware de los mismos.

Artículo 8. Implementación de Redes de Datos. La División de Desarrollo Informático, por medio del Departamento de Infraestructura y Telecomunicaciones es la única área autorizada para implementar o darle mantenimiento a la red de datos Institucional, tomando en consideración lo siguiente:

a) El tipo de cable a utilizar debe cumplir con las especificaciones para Categoría 6A como mínimo, estipuladas en las normas ANSI/TIA-568-C.2.

b) Todos los cables de par trenzado balanceado de categoría 6A o superior deben probarse conforme a la norma ANSI/TIA-568-C.2, en la medida de lo posible o certificar como mínimo su conectividad.

c) Las canalizaciones tanto horizontales como verticales deben instalarse y diseñarse de tal modo que puedan mantenerse los radios mínimos de curvatura especificados por el fabricante para los cables horizontales y verticales.

d) Todas las salidas/conectores de telecomunicaciones deben ser categoría 6A, estar diseñadas para la terminación de cable de cobre de par trenzado balanceado categoría 6A o a la categoría del cable de cuatro pares más actualizada, que pueda certificarse y esté disponible en el mercado.

CAPÍTULO III
INTERNET Y CORREO ELECTRÓNICO

Artículo 9. Administración de Internet y Correo Electrónico. Los servicios de internet y correo electrónico, son administrados por la División de Desarrollo Informático quien es la responsable de garantizar su disponibilidad. La División de Desarrollo Informático, a consideración de la Gerencia que lo requiera, monitoreará las actividades de la red, tanto para correo electrónico, internet y uso de red de datos con el fin de vigilar el cumplimiento de las políticas establecidas para su uso.

Artículo 10. Conexión a Internet. La División de Desarrollo Informático, por medio del Departamento de Infraestructura y Telecomunicaciones tiene la gestión de un canal de acceso a Internet, el cual debe ser distribuido de acuerdo a las necesidades establecidas por la División. El canal debe ser de uso exclusivo de la Institución y debe ser utilizado para:

a) Puesta en marcha de los servicios de ***inde.gob.gt*** que sean publicados en el Internet, para brindar acceso a los sistemas Institucionales. El dominio y subdominios de **inde.gob.gt** a partir de la entrada de vigencia del presente Normativo, quedan bajo la administración de la División de Desarrollo Informático.

b) Para la transferencia de mensajería de correo electrónico en Internet.

c) Para la navegación de usuarios autorizados en Internet, cuya información consultada esté relacionada con la naturaleza propia de sus funciones.

d) Para actualización en línea de los servicios o aplicativos de software de red, que necesite constantemente actualizarse.

e) Para la publicación del servicio de DNS, el cual contiene los registros de nombres de dominio.

Artículo 11. Correo Electrónico: El correo electrónico es proporcionado con el objeto de apoyar las funciones de comunicación de la Institución y debe contar con las siguientes características:

a) La dirección de correo electrónico de cada usuario estará formada por una inicial del nombre y el apellido del usuario, salvo excepciones (xapellido@inde.gob.gt).

b) Los buzones de correo electrónico, son propiedad de la Institución, por tanto, también toda información contenida en ellos, su uso debe ser para temas exclusivamente laborales.

c) Las comunicaciones Institucionales efectuadas por correo electrónico, solo podrán ser realizadas por las cuentas Institucionales.

d) Los usuarios son los únicos responsables de todas las actividades realizadas, desde sus cuentas de correo y buzones.

e) La cuenta de correo es intransferible, por lo que no debe proporcionarse a otras personas.

CAPÍTULO IV
SOFTWARE

Artículo 12. Administración de Software. La División de Desarrollo Informático, será la única área encargada de la administración, instalación, soporte, documentación y funcionamiento del software autorizado y permitido de acuerdo a lo establecido en las políticas de Directorio Activo (Active Directory) en la Institución, sea web o de escritorio. Dentro de las responsabilidades de la administración e instalación de software se describe las siguientes:

a) Mantener bajo resguardo las licencias de uso de software de la Institución, además de llevar un control de las licencias que se encuentran en operación y uso.

b) Mantener actualizado el catálogo de software (libre o propietario) de la Institución.

c) Desinstalar el software de las computadoras que no posean licencias, con el propósito de no infringir la Ley de Derecho de Autor y Derechos Conexos y sus Reformas.

d) Previa la instalación de software libre en los equipos, se debe verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de este tipo de software.

e) Generación de estándares de software Institucional, antes de ser entregados al usuario final).

f) Creación de estándares de software adicional, que será de uso exclusivo del INDE, entre los cuales se pueden encontrar los siguientes:

i. Software preinstalado en el equipo de cómputo.
ii. Software de acceso a componentes en los servidores de la Institución.
iii. Software de uso emergente (previo análisis de licencia y seguridad).
iv. Generación de estándares de software de soporte (sistema informático que viene junto a la adquisición de un artículo como cámaras, IPAD, periféricos, etc.)

g) En la administración de software no se podrá instalar lo siguiente:

i. Copias ilegales de cualquier sistema informático, software o programa.
ii. Software descargado desde internet.
iii. Software que no haya sido aprobado por la División de Desarrollo Informático.
iv. Software adquirido para uso personal sin fines Institucionales.
v. Software de entretenimiento.

Si un usuario incurre en abuso de los permisos otorgados o es parte de la propagación o infección de virus a su computadora o a la Red Institucional, es responsable por las posibles consecuencias de este hecho al comprobarse el mismo por medio de una Auditoria de Sistemas, aplicándole lo indicado en el Articulo 5, literal o).

CAPÍTULO V
PROPIEDAD INTELECTUAL DE LA INFORMACIÓN

Artículo 13. Propiedad de la Información: Los datos que se crean y/o modifican en todos los sistemas, aplicaciones y cualquier otro medio de procesamiento electrónico sea disco duro interno o externo, memoria flash, etc., durante el desarrollo normal de las actividades laborales, son propiedad de la Institución considerando lo siguiente:

a) Los derechos de autor de un software, hojas de cálculo, archivos PDF o tipo de documentos, macros, base de datos, etc., y su respectiva documentación, creados por los trabajadores en ejercicio de sus actividades laborales, son de absoluta exclusividad y propiedad del INDE.

b) La División de Desarrollo Informático será la encargada de resguardar los respaldos que tengan información de actividades laborales del INDE y que fueron realizados o solicitados por los trabajadores.

CAPÍTULO VI
SEGURIDAD DE LA RED PERIMETRAL

Artículo 14. Firewall de Perímetro para Conexión de Redes Externas. La División de Desarrollo Informático debe considerar la implementación de una barrera entre la red perimetral y la red interna de la Institución, por lo que debe tener instalado al menos un firewall, el cual se encargará de garantizar control de acceso de tráfico desde y hacia Internet. Este dispositivo permitirá esconder todos los recursos de la red interna actuando como una barrera perimetral y deje publicar los servicios de la Institución, mensajería de correo electrónico y resolución de nombres. También debe permitir la salida de tráfico que se origine desde la red interna hacia Internet, principalmente para la navegación de usuarios, garantizando que los usuarios puedan tener acceso a los recursos externos de Internet de forma tal que no comprometa la seguridad de los recursos informáticos de la red interna. El Departamento de Infraestructura y Telecomunicaciones de la División de Desarrollo Informático debe considerar que los equipos incluyan como mínimo las siguientes funcionalidades:

a) Firewall de tecnología cortafuego stateful independiente de sistema operativo convencional.

b) Sistema de traducción de direcciones estática y dinámica.

c) Capacidad para registrar eventos del sistema y generación de reportes.

d) Capacidad para ser manejado por medio de un software de definición de políticas de seguridad.

e) Capacidad de reglas de tráfico IP.

f) Soporte de filtros de contenido Web (ActiveX, Applets, etc.) para protección de los usuarios internos.

g) Autenticación, autorización y auditoría de usuarios.

h) Soporte de actualización del sistema operacional para mejoras de funcionalidad y protección de vulnerabilidades.

i) Capacidad de adaptarse a esquema de conmutación por error (failover).

j) Respaldo y recuperación de la configuración del sistema.

k) Establecimiento de un programa que permita mantener actualizado los dispositivos con suscripciones anuales, para el adecuado funcionamiento y establecimiento de estándares y normas de acuerdo a las actualizaciones de cada fabricante.

Artículo 15. Accesos y Conexiones a través de una Red Privada Virtual (VPN). El acceso remoto a través de una red VPN, se debe realizar usando firewalls destinados para la interconexión, utilizando los protocolos adecuados y respetando las normas siguientes para la protección de la información Institucional:

a) Para cada caso y si lo amerita la División de Desarrollo Informático debe revisar la factibilidad técnica para resolver necesidades de acceso desde el exterior utilizando esta tecnología.

b) El servicio aplica a quienes requieren acceder (justificadamente y cuando no exista alternativa alguna) desde el exterior a los recursos de información publicados en la Intranet de la Institución.

c) Para utilizar este servicio se debe cumplir con los siguientes requisitos:

i. Solicitud y autorización por escrito del Jefe Inmediato
ii. Justificación del motivo por el cual requiere el acceso.
iii. Especificación de los servicios que deben pasar a través del túnel de VPN.
iv. Autorización o acuerdo interinstitucional (cuando aplique) que avale la interconexión, detallando los recursos que serán compartidos a través del túnel de VPN
v. Especificar la duración de la conexión a los sistemas y recursos de la Institución.

d) El tiempo hábil del servicio de VPN no puede superar los 6 meses. Al cabo de este tiempo el acceso debe ser deshabilitado. Antes de la expiración de los permisos otorgados, la dependencia o Institución autorizada debe revalidar los accesos, solicitando la extensión del servicio, la cual no puede ser mayor al tiempo establecido en la presente política y debe realizarse con 5 días de anticipación al vencimiento del servicio.

CAPÍTULO VII
ASEGURAMIENTO DEL DESEMPEÑO DE LA RED

Artículo 16. Protección Antivirus. La División de Desarrollo Informático, es la encargada y responsable de la implementación de la solución antivirus y antimalware en los equipos informáticos de la Institución, observando lo siguiente:

a) Se debe contar con una plataforma corporativa con la que se pueda administrar y monitorear las actualizaciones de las firmas de virus y que estas sean distribuidas de forma automática por una plataforma centralizada.

b) Todos los equipos informáticos del INDE y sus Empresas deben contar con la última versión actualizada de la solución antivirus o antimalware que la Institución tenga con licenciamiento vigente.

c) La solución antivirus y antimalware debe ser capaz de proteger al sistema operativo en tiempo real y de actualizarse de forma automática, sin que esto afecte el óptimo desempeño de la red interna y de los sistemas informáticos Institucionales.

d) En caso de presentarse una alarma o alerta de la solución antivirus por infección de virus o malware se debe informar a la División de Desarrollo Informático, quien por medio del Departamento de Soporte Técnico debe proceder a realizar la revisión y limpieza correspondiente. Si el personal del Departamento de Soporte Técnico no puede realizar la limpieza satisfactoriamente se debe desconectar el equipo informático de la red interna de la Institución, para evitar que el virus o malware se propague a mas equipos en el ámbito de red donde se encuentra el equipo informático afectado, y este debe ser trabajado en un área provista para el efecto con el apoyo de técnicos de la solución de antivirus.

e) La versión de antivirus y antimalware debe ser específica para la plataforma de sistema operativo que tienen los servidores de la Institución, la cual no debe afectar los servicios, aplicaciones o recursos que sean administrados por estos equipos informáticos.

CAPITULO VIII
PROHIBICIONES

Artículo 17. Prohibiciones. Las siguientes actividades se consideran no aceptables, ya sea por dolo, desconocimiento u omisión en virtud de que ponen en riesgo la continuidad y la seguridad de los servicios de conectividad de la Institución:

a) No está permitido la instalación de equipos activos como hub, switches no administrables, routers y puntos de acceso inalámbrico en los puntos de red que provee la Institución.

b) El uso inapropiado del canal de Internet por parte de algún usuario de la red será registrado y notificado el hecho al jefe inmediato.

c) Utilizar la Infraestructura de conectividad para cometer ilícitos o acceder a información no permitida.

d) Navegar por Internet en sitios ajenos a las labores Institucionales.

e) Enviar y recibir correos de cuentas personales que contengan información no propia de las actividades Institucionales.

f) Envío o reenvío por medio del correo electrónico Institucional de toda publicidad, correo no solicitado (spam) o cualquier tipo de aviso comercial, que pudiera saturar los canales de comunicación o los buzones de los usuarios.

g) El envío por medio del correo Institucional de contenido ilegal por naturaleza o que constituya complicidad con hechos delictivos. Por ejemplo, material ofensivo, pornográfico, amenazas, estafas, difamaciones, racista u obsceno, etc.

h) La difusión vía correo de mensajes contrarios a la moralidad, las buenas costumbres, racistas, antinacionalistas o todos aquellos que puedan atentar contra las personas o las instituciones.

i) Participar en la propagación de cadenas, esquemas piramidales y otros similares de envío con el correo Institucional.

j) Enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.

k) Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad del emisor del correo electrónico.

l) Ofrecer su cuenta de correo electrónico a personas no autorizadas.

m) Atentar contra la seguridad del servidor de correo de la institución.

n) Descargar o instalar todo tipo de archivos ajenos a las labores Institucionales, como pueden ser fotos, videos, música, o programas (incluyendo los de descarga masiva de material de entretenimiento).

o) Conexión de dispositivos de almacenamiento externo que permitan extraer información alguna de la Institución.

p) Conexión de dispositivos que permitan la conexión hacia o desde otra red de datos que no sean las autorizadas por la División de Desarrollo Informático por ejemplo Internet.

q) Propagar o ejecutar de forma intencionada en los equipos informáticos de la Institución, software, o algún código malicioso que este diseñado para replicar, dañar, espiar o alterar el desempeño de cualquier sistema o equipo informático.

r) Cualquier tipo de sabotaje orientado a hacer fallar los servicios o sistemas informáticos, saturar los buzones de correo, inhabilitar o engañar a un usuario determinado.

s) Hacerse pasar por otro trabajador o usurpar una cuenta de usuarios de red (dominio), correo electrónico, sistema auxiliar o cualquier otro sistema informático.

t) Cualquier intento de sondear, rastrear, examinar o probar las vulnerabilidades de la Red Institucional, así como romper los límites de seguridad o medidas de autenticación.

u) Alterar los encabezados o el contenido de cualquier paquete de comunicación o de cualquier parte de información en un mensaje de correo electrónico.

v) El uso de programas que puedan distraer la labor de los usuarios y que puedan causar saturaciones en los servicios de red, incluyendo los que permiten mensajes interactivos.

w) Tratar de descifrar, averiguar o adquirir las claves de otros usuarios.

x) Conectar redes independientes a la Red Institucional, por medio de la conexión de equipos de red activos (hubs, switches, routers, módems, firewalls, puntos de acceso inalámbricos, entre otros) que previsiblemente perturbe el correcto funcionamiento de esta o comprometa su seguridad, salvo expresa autorización de la División de Desarrollo Informático.

y) Compartir información de cualquiera de los sistemas implementados en la Institución para efectos que no corresponda a las actividades propias del trabajo

Institucional, sea esta extraída por cualquier medio (capturas de pantalla, impresión de documentos, fotografías, archivos digitales, etc.) y distribuirlos en redes sociales, correos electrónicos fuera de la Institución con fines maliciosos o desconocidos. Para el efecto debe utilizar los medios de comunicación oficiales para el traslado de información (oficina de acceso a la información pública) o bien dirigirse a la unidad respectiva para la emisión de las respectivas certificaciones válidas y autorizadas.

z) Adquirir equipos denominados "Todo en Uno" de escritorio, por ser equipos compactos, que tienen un menor sistema de ventilación y sus componentes pueden presentar desperfectos por lo delicado de los mismos, haciéndolos obsoletos en un menor tiempo del esperado.

aa) Adquirir componentes o accesorios (pantallas, periféricos, dispositivos de lectura de datos, etc.) que no incluyan los cables o adaptadores necesarios para su conexión, debiendo además determinar si el equipo al cual se desea conectar tiene la capacidad o cuenta con los medios para dicha conexión (tarjetas o puertos).

ab) Adquirir impresoras personales. Se debe priorizar la compra de impresoras multifuncionales para uso de todo el personal de una Unidad o Departamento, se debe contemplar el mantenimiento de al menos 3 años por parte del distribuidor o fabricante, además que sea provisto por cualquier medio físico (USB, CD, DVD) el software necesario para su funcionamiento y este sea compatible con el o los sistemas operativos de uso de la Institución.

ac) Adquirir equipo de cómputo que posea licencia de sistema operativo y software ofimático edición Home, si dicho equipo se desea utilizar en la Red Institucional, deben ser proporcionadas licencias ediciones Enterprise o Professional, por el proveedor seleccionado.

CAPÍTULO IX
DISPOSICIONES FINALES

Artículo 18. Casos No Previstos. Los casos no previstos en el presente normativo deben ser resueltos por la Gerencia General, a solicitud de la División de Desarrollo Informático.

Artículo 19. Incumplimiento. El incumplimiento a las disposiciones establecidas en el presente normativo, se considera como una infracción laboral y debe ser sancionado en conformidad a lo regulado en el Pacto Colectivo de Condiciones de Trabajo INDE-STINDE.

Artículo 20. Derogatoria. Queda derogado el Normativo para Administrar la Red del INDE y sus Componentes, aprobado mediante Acuerdo Número GG-A-41-2017, así como las disposiciones internas que se opongan o contradigan lo dispuesto en el presente Normativo.

Artículo 21. Vigencia. El presente Normativo, fue aprobado el 19 de agosto del 2021; y entra en vigencia al día siguiente de su publicación en la Intranet de la Institución.

INSTITUTO NACIONAL DE ELECTRIFICACIÓN GERENTE GENERAL INDE GUATEMALA C.A.

ING. OTTO LEONEL GARCÍA MANSILLA
GERENTE GENERAL