CO – DIRECCIÓN, INSTITUTO NICARAGÜENSE DE ESTUDIOS TERRITORIALES (INETER).
LIBRO DE RESOLUCIONES ADMINISTRATIVAS AÑO 2020

RESOLUCIÓN ADMINISTRATIVA No. 105-2020
"APROBACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL INSTITUTO NICARAGUENSE DE ESTUDIOS TERRITORIALES, INETER"

El suscrito, Co - Director de Vigilancia de los Fenómenos Naturales del Instituto Nicaragüense Estudios Territoriales (INETER) en uso de las facultades que le confiere la Constitución Política de la República de Nicaragua y sus reformas, Ley 290, "Ley de Organización, Competencia y Procedimientos del Poder Ejecutivo", Reglamento de la Ley 290 (Decreto 71-98, del 30 de Octubre de 1998), la Ley Orgánica de INETER, Ley 311, publicada en La Gaceta, Diario Oficial, No. 143 del 28 de Julio de 1999 y su reglamento, Decreto Número 120-99, publicado en La Gaceta, Diario Oficial No. 229, del día 30 de noviembre de 1999; atribuciones conferidas en la Ley No. 825, Ley de Reforma a la Ley No. 311, Ley Orgánica del Instituto Nicaragüense de Estudios Territoriales (INETER), publicada en La Gaceta, Diario Oficial, No. 05, del 11 de Enero del año 2013 y finalmente las facultades conferidas en la Ley 681, Ley Orgánica de la Contraloría General de la Republica y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, así como las Normas Técnicas de Control Interno publicadas en La Gaceta, Diario Oficial número 67 del 14 de abril del 2015, respectivamente.

CONSIDERANDO:

I.

Que es necesario fortalecer el control previo para prevenir los actos que puedan afectar negativamente la efectividad y transparencia en la administración de los bienes y recursos del estado.

II.

Que en cumplimiento a lo establecido en la Ley No. 681, Ley Orgánica de la Contraloría General de la República y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes del Estado, publicada en La Gaceta, Diario Oficial con No. 113 del día 18 de junio del año dos mil nueve, respectivamente, y las Normas Técnicas de Control Interno aprobadas por el Consejo Superior de la Contraloría General de la República, publicadas en La Gaceta, Diario Oficial con No. 67 del día 14 de marzo del año dos mil quince.

III.

Que el control interno es complementario del control externo de la Contraloría General de la República, entidad fiscalizadora que con sujeción a su Ley Orgánica, podrá evaluar, orientar, coordinar, y en caso necesario, dispondrá los sistemas de control interno de los organismos y entidades que conforman el sector público, siendo esta normativa, un instrumento a utilizar, en cumplimiento de las funciones establecidas en el artículo 31 del reglamento de la Ley Orgánica,

Ley No. 311, le corresponde coordinar y regular la sistematización de las bases de datos institucionales y los sistemas geográficos sectoriales, para su adecuada utilización, así como de resguardar la información básica y documental institucional y en cumplimiento a las Normas técnicas de control interno, en su apéndice 9.1, "Actividades de control aplicables a los sistemas de administración" todo sistema de información debe ser controlado para asegurar el funcionamiento y confiabilidad del procesamiento de las transacciones efectuadas, que detalle la correspondencia de sus actividades, con los objetivos y estrategias de la misma.

IV.

Por lo que se hace necesario para INETER, contar con un documento en el cual estén consignadas en forma metódica, los procedimientos que debe implementar la Dirección General de Sistemas Geoinformáticos del INETER, para coadyuvar al apoyo en la realización del cotidiano quehacer institucional, corresponde a la máxima autoridad dar el seguimiento adecuado que permita asegurar la implantación oportuna de las recomendaciones que hace la Contraloría General de la República, para fortalecer el control y la transparencia en los actos administrativos del sector público.

V.

La Seguridad Informática es un aspecto de especial importancia para cualquier organización, cuyas operaciones se soportan en servicios informático y tecnología. Una administración eficiente de los recursos informáticos ayuda a mejorar la Seguridad Informática y la confianza del usuario en los sistemas informáticos sólo se puede lograr a través de una protección efectiva de los diferentes elementos que se integran en las plataformas de cómputo y comunicaciones que sirven para administrar, procesar e intercambiar la información.

VI.

Estos ambientes informáticos han sido sometidos a una constante evolución que permanentemente modifica las condiciones de trabajo de los sistemas y genera la aparición de nuevos riesgos y amenazas que deben atenderse para minimizar los efectos potenciales que puedan tener sobre la organización. Esta necesidad ha motivado el desarrollo del presente documento de políticas para la Seguridad Informática que se orientan principalmente al uso adecuado de las destrezas tecnológicas, hacer recomendaciones para obtener el mayor provecho de la tecnología y evitar su uso indebido, ya que esto puede ocasionar serios problemas a los bienes, servicios y operaciones del INETER.

Por tanto en uso de las facultades que se me confieren;

POR TANTO ESTA AUTORIDAD:

En uso de las facultades que me confiere los artículos 130 y 131 de nuestra Constitución Política, artículos 1, 2, de Ley N°. 311, "Ley Orgánica del Instituto Nicaragüense de Estudios

Territoriales (INETER)", Reglamento a la Ley No.311, Ley Orgánica del Instituto Nicaragüense de Estudios Territoriales. (INETER), atribuciones conferidas en los artículos 11, 12 y 13 de la Ley No. 825, Ley de Reforma a la Ley No. 311, Ley Orgánica del Instituto Nicaragüense de Estudios Territoriales (INETER); y el artículo 14 de la Ley No.290, Ley de Organización, Competencia y Procedimientos del Poder Ejecutivo, definen las atribuciones de la Dirección Superior del Instituto Nicaragüense de Estudios Territoriales (INETER), como un ente descentralizado con autonomía técnica y autonomía administrativa y finalmente las facultades conferidas en la Ley 681, Ley Orgánica de la Contraloría General de la Republica y del Sistema de Control de la Administración Pública y Fiscalización de los Bienes y Recursos del Estado, así como las Normas Técnicas de Control Interno publicadas en La Gaceta, Diario Oficial número 67 del 14 de abril del 2015 el Co-director de INETER,

ACUERDA:

PRIMERO: Aprobar el documento denominado; **"POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL INSTITUTO NICARAGUENSE DE ESTUDIOS TERRITORIALES, INETER",** que servirá de base para el desarrollo de las funciones y procedimientos que debe implementar la Dirección General de Sistemas Geoinformáticos y demás áreas institucionales en el INETER, este documento es de aplicación y estricto cumplimiento para toda la entidad.

SEGUNDO: Este documento podrá estar sujeto a cambios de acuerdo a ajustes de la política que establezcan para el sector público y entrará en vigencia a partir de la fecha de autorización y divulgación a las partes involucradas.

TERCERO: Comuníquese la presente Resolución Administrativa a cuantos corresponda conocer de la misma.

Dado en la ciudad de Managua a las una y quince minutos de la tarde del día seis de agosto del año dos mil veinte.

Federico Vladimir Gutiérrez Corea, Ph.D.
Co-Director de Vigilancia de los Fenómenos Naturales, INETER.

Daniel, Buen Gobierno
Nicaragua: Cristiana, Socialista y Solidaria

2020

Políticas de Seguridad Informática para el INETER

DIRECCIÓN GENERAL DE SISTEMAS GEOINFORMÁTICOS

Control de cambios

Versión	Fecha	Descripción	Autor
1	14-jul-2020	Definición de estructura del documento, metodología de trabajo y cronograma.	DGSGI/DGCF
2	15-jul-2020	Definición de medidas tomadas a nivel de Infraestructura Tecnológica	DGSGI/DGCF
3	16-jul-2020	Definición de medidas tomadas a nivel de Sistemas de Información	DGSGI/DGCF
4	17-jul-2020	Definición de medidas tomadas a nivel de bases de datos	DGSGI/DGCF
5	22-jul-2020	Creación de glosario técnico	DGSGI
6	27-jul-2020	Homologación de aportes y estructuración del documento	DGSGI
7	30-jul-2020	Revisión final de parte del Comité de Seguridad Informática	DGSGI

Tabla de contenido

Instituto Nicaragüense de Estudios Territoriales - INETER - Dir. Gral. de Sistemas Geoinformáticos

I.- Introducción.

La Seguridad Informática es un aspecto de especial importancia para cualquier organización, cuyas operaciones se soportan en servicios informático y tecnología. Una administración eficiente de los recursos informáticos ayuda a mejorar la Seguridad Informática y la confianza del usuario en los sistemas informáticos sólo se puede lograr a través de una protección efectiva de los diferentes elementos que se integran en las plataformas de cómputo y comunicaciones que sirven para administrar, procesar e intercambiar la información.

Estos ambientes informáticos han sido sometidos a una constante evolución que permanentemente modifica las condiciones de trabajo de los sistemas y genera la aparición de nuevos riesgos y amenazas que deben atenderse para minimizar los efectos potenciales que puedan tener sobre la organización. Esta necesidad ha motivado el desarrollo del presente documento de políticas para la Seguridad Informática que se orientan principalmente al uso adecuado de las destrezas tecnológicas, hacer recomendaciones para obtener el mayor provecho de la tecnología y evitar su uso indebido, ya que esto puede ocasionar serios problemas a los bienes, servicios y operaciones del INETER.

Por ello las presentes Políticas para la Seguridad Informática se plantean como una herramienta organizacional para alinear esfuerzos y crear conciencia entre los colaboradores y usuarios del Instituto, sobre la importancia de mantener protegidos la información y los servicios tecnológicos que soportan las funciones del INETER. En este documento se propone una política de Seguridad Informática que requiere un alto compromiso con el Instituto, agudeza técnica para establecer fortalezas y detectar debilidades en su aplicación, y constancia para mantenerla actualizada de forma continua en función de los cambios tecnológicos que la influyen.

Así como la tecnología y las amenazas a los entornos digitales cambian tan rápidamente, las políticas y lineamientos en materia de seguridad deben adaptarse a ese constante cambio. Por lo tanto, este documento debe obligatoriamente actualizarse constantemente. La Dirección General de Sistemas Geoinformáticos es el área responsable de la elaboración, actualización de la Política. El cumplimiento es una responsabilidad conjunta entre las autoridades de la institución y los usuarios (internos y externos).

II.- Glosario.

Para efectos de las presentes Políticas se entenderá por:

Activos Informáticos: Comprenden a los recursos informáticos tales como equipos de cómputo, los equipos de comunicaciones, el software, las bases de datos e información no estructurada que deben ser protegidos por el ambiente de Seguridad Informática del Instituto;

Ambiente de Desarrollo: Área donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. Este entorno es de uso exclusivo del personal de la Dirección de Desarrollo de Software;

Ambiente de Producción: Área donde se ejecutan los sistemas y se encuentran los datos de producción. Es decir, los datos generados por los sistemas de información ejecutados por las áreas dueñas de cada sistema y sus usuarios;

Ambiente de Seguridad Informática: Medidas de Seguridad Informática que se establecen en el INETER, con la finalidad de proteger sus activos informáticos, crear conciencia de la seguridad, incrementar el compromiso de su personal y garantizar la continuidad de las actividades del Instituto;

API (*Application Programming Interface*, Interfaz de Programación de Aplicaciones): Conjunto de reglas (código) y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas.

Áreas de Acceso Restringido: Comprenden las áreas de centro de datos, de suministro de energía eléctrica, de aire acondicionado, cuarto de máquinas, racks de comunicaciones, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas Electrónicos;

Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del Usuario y el Instituto;

Base de Datos: Conjunto organizado de datos con relaciones predefinidas entre ellos, es decir base de datos relacional.

Comité de Seguridad Informática: Estructura organizacional ad-hoc conformada por el Responsable de la Dirección General de Sistemas Geoinformáticos, los Directores Específicos de la DGSGI y aquellos especialistas en la materia cuyos aportes se consideren oportunos, para coordinar los aspectos y medidas necesarias relacionadas con la Seguridad Informática para garantizar la continuidad de las funciones del Instituto;

Confidencialidad: Principio de la seguridad de la información que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma;

Control de Acceso: Orientado a controlar el acceso lógico a la Información Electrónica;

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades que permite estudiarlos, analizarlos o conocerlos. Un dato por sí mismo no constituye información, es el procesamiento de los datos lo que nos proporciona información.

DBA: Administrador de Bases de Datos (Database Administrator).

DDL: Lenguaje de Definición de Datos (Data Definition Language), cuyas sentencias se utilizan para crear, modificar o borrar objetos de las bases de datos.

DDS: Dirección de Desarrollo de Software Geoinformático

DGI: Dirección de Georepositorio Institucional.

DGSGI: Dirección General de Sistemas Geoinformáticos;

Disponibilidad: Principio de la seguridad de la información que garantiza que los Usuarios autorizados tengan acceso a la información o a los recursos relacionados con la misma, toda vez que lo requieran;

DIT: la Dirección Infraestructura Tecnológica;

DML: Lenguaje de Manipulación de Datos (Data Manipulation Language), cuyas sentencias son utilizadas para crear, editar o borrar registros en la estructura de las bases de datos.

Evaluación de Riesgos: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las Instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación del Instituto;

Información electrónica institucional: La información en formato electrónico o asimilable directamente a través de un recurso informático que por su contenido resulte sensible, necesaria o valiosa para el desempeño de las funciones y obligaciones del INETER;
Información electrónica sensible: La información en formato electrónico o asimilable directamente a través de un recurso informático que sea valiosa para el Instituto y que deba ser protegida por ser confidencial y/o necesaria para la continuidad operativa o la realización de las funciones de una o varias áreas del INETER, la consecución de sus objetivos, o el cumplimiento de la normatividad vigente;

Infraestructura Tecnológica de Seguridad Informática: Conjunto de metodologías y herramientas informáticas que permiten proteger los sistemas y servicios informáticos del INETER, detectar amenazas informáticas y garantizar la continuidad de las actividades del Instituto;
Instituto o INETER: el Instituto Nicaragüense de Estudios Territoriales;

Integridad: Principio de la seguridad de la información que garantiza y salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento;

NAS (Network Attached Storage, Almacenamiento Conectado a la Red): Es una arquitectura de almacenamiento a nivel de archivos en la que uno o más servidores almacenan datos en discos dedicados y los comparten con muchos clientes conectados a la red.

No repudio: Se refiere a evitar que una persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió;

Planes de continuidad: Es la planificación que identifica el Instituto ante la exposición de amenazas internas y externas que ofrecen una prevención de recuperación de las operaciones del INETER, manteniendo la integridad de los sistemas y servicios informáticos, y su información.

RAID (Redundant Array of Independent Disks): Arreglo de discos redundante, es una tecnología de discos que permite guardar la misma información en diferentes lugares en múltiples discos, con el objetivo de incrementar la tolerancia a fallas y la tener alta disponibilidad.

Recurso Informático: Recurso (tangible o intangible) o servicio que sea necesario para apoyar tareas relacionadas con la captación, el almacenamiento, el procesamiento, el acceso o la transmisión de información o datos utilizando medios electrónicos, ópticos o magnéticos;

Repositorio: Es un depósito o almacén digital centralizado donde se almacena y mantiene información digital, en bases de datos o datos no estructurados.

Respaldo / Backup: Es la copia de información a un medio del cual se pueda recuperar y restaurar la información original.

Riesgo: Combinación de la probabilidad de un suceso y sus consecuencias negativas.
Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Seguridad en el Desarrollo y Mantenimiento de los Sistemas: Proceso orientado a garantizar la incorporación de medidas de seguridad en los Sistemas de Información desde su desarrollo hasta su implementación y mantenimiento;

Servicio Informático: Conjunto de las funcionalidades, reglas y recursos informáticos que sirven para satisfacer las necesidades usuarios internos y externos del Instituto en un aspecto específico del campo de la informática o de las comunicaciones;

Servicio Web: Colección de protocolos abiertos y estándares usados para intercambiar datos entre aplicaciones o sistemas a través de una red.

Soporte Móvil de Almacenamiento Informático removible: Comprenden a los discos externos, Pendrive, Tarjetas de Memorias, DVD´s, CD´s, cintas magnéticas, etc.;

Usuario de Sistemas y Servicios Informáticos: Al personal perteneciente al Instituto o a una organización con la que este tenga convenio, que haga uso de bienes, servicios, recursos informáticos o de información electrónica que sea

Usuario Externo: Funcionario de organizaciones con las que el INETER tenga convenios de intercambio de datos o población en general que consulte los datos publicaos por el Instituto en sus distintos canales de difusión.

VLAN (*Virtual Local Area Network*): Red lógica independiente dentro de una misma red física.

Instituto Nicaragüense de Estudios Territoriales - INETER - Dir. Gral. de Sistemas Geoinformáticos

III-. Objeto.

Establecer la política institucional en materia de Seguridad Informática que apoye la Seguridad de la Información, entendida como la preservación de su integridad, confidencialidad y disponibilidad, así como instrumentar y coordinar acciones para minimizar daños a la infraestructura tecnológica y a los sistemas informáticos.

IV.- Marco Jurídico.

A. Constitución Política de la República de Nicaragua.
B. Leyes.
   1. Ley 311. Ley Orgánica del Instituto Nicaragüense de Estudios Territoriales (INETER).
   2. Ley 509. Ley General de Catastro Nacional.
   3. Ley 641, Código Penal.

C. Normativas Internas
   1. Manual de Procedimiento de la Dirección General de Sistemas Geoinformáticos
   2. Normativa de Resguardo de Información No Estructurada

V.- Políticas Generales.

A.- Organización de la Seguridad Informática.

1.- El objetivo principal de la Seguridad Informática será proteger desde el ámbito tecnológico los activos informáticos de la institución, tanto digitales como físicos, y los servicios tecnológicos necesarios para que el INETER pueda cumplir con las funciones y obligaciones que le correspondan de acuerdo a la legislación nacional aplicable.

2.- La Seguridad Informática en el INETER implica una responsabilidad compartida por parte de los administradores y usuarios de Equipos, Sistemas y Servicios Informáticos Institucionales.

3.- La DGSGI es el área responsable de coordinar acciones; determinar la Infraestructura Tecnológica; y establecer lineamientos, estándares, criterios, medidas y otras disposiciones técnicas, en materia de Seguridad Informática.

4.- El titular de la DGSGI coordinará con los directores específicos de la DGSGI y personal técnico que estime oportuno las estrategias y líneas de acción en términos de la Seguridad Informática del INETER, formando así un comité ad-hoc de seguridad informática.

5.- El comité de seguridad informática del INETER, tendrá las siguientes responsabilidades:

a) Proponer e integrar estrategias y elementos para conformar las políticas y normativas en temas de Seguridad Informática, en coordinación con las autoridades y los Directores Generales del INETER;

b) Establecer acuerdos en materia de Seguridad Informática con áreas internas e instituciones externas al INETER;

c) Proponer recomendaciones y acciones de aplicación general en materia de Seguridad Informática;

d) Proponer criterios para la clasificación, registro y protección de los recursos informáticos del INETER, desde el punto de vista de la Seguridad Informática;

e) Proponer especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática que sean aplicables a cualquiera de los elementos tecnológicos que integren la Infraestructura de Seguridad Informática del INETER;

f) Garantizar que se publiquen en la Intranet Institucional los documentos normativos en materia de Seguridad Informática emitidos por la DGSGI y aprobados por la Dirección Superior del INETER;

g) Promover el cumplimiento de la normatividad informática en el INETER;

h) Proponer y operar sistema de gestión de incidentes, en el cual se sistematizarán aquellos eventos de falla de cualquier elemento de la infraestructura que amenace los principios de la Seguridad Informática;

i) Coordinar las acciones inmediatas para manejar los reportes de incidentes y anomalías de Seguridad Informática;

j) Analizar aquellos incidentes que involucren los servicios informáticos a fin de establecer controles para detectar, corregir y prevenir incidentes posteriores;

k) Determinar y mantener actualizado el inventario de Activos Informáticos relacionados con la Infraestructura de Seguridad Informática;

l) Realizar revisiones selectivas a los controles de los activos informáticos para asegurar que se mantenga sobre ellos la aplicación de las recomendaciones y lineamientos en materia de Seguridad Informática;

m) Mantener un sistema de monitoreo y seguimiento del desempeño del ambiente de Seguridad Informática;

n) Definir e implementar controles de detección y prevención para la protección contra software malicioso en la infraestructura de cómputo y telecomunicaciones;

o) Designar las Áreas de Acceso Informático Restringido y establecer medidas para el control de acceso físico y lógico;

p) Almacenar y administrar las credenciales de acceso incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados;

q) Revocar credenciales de acceso a sistemas y servicios informáticos, cuando las mismas estén comprometidas o cuando un usuario que haga uso de ellas se desvincule del INETER;

r) Recuperar las claves perdidas o alteradas como parte de la administración para su continuidad;

s) Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles en la red local del INETER;

t) Controlar y registrar todos los certificados de seguridad de los sitios y servidores del INETER;

u) Analizar en conjunto con la DISUP los riesgos de los accesos de terceros a la información del INETER y proponer medidas con el propósito de minimizar sus posibles efectos;

v) Elaborar, implementar y dar seguimiento a Planes de Continuidad necesarios para atender eventualidades que puedan afectar la continuidad de las operaciones del INETER;

w) Coordinar las tareas definidas en los Planes de Continuidad; y

x) Realizar ensayos, mantenimiento y reevaluación de los Planes de Continuidad.

y) Reunirse periódicamente para actualizar la documentación normativa relativa a la seguridad informática.

B.- Administración de los Activos Informáticos.

1.- La DGSGI a través de la DIT deberá diseñar, implementar y mantener un inventario actualizado de los Activos Informáticos relacionados con la Infraestructura de Seguridad Informática del INETER.

2.- En materia de Administración de los Activos la DIT deberá mantener la información actualizada de los activos de los cuales sean responsables. Asimismo, establecer esquemas de protección del activo acordes a las recomendaciones, políticas y lineamientos que sean emitidos por el comité de Seguridad Informática.

C.- Responsabilidades en Materia de Seguridad Informática para el Uso de Bienes, Servicios, Recursos Informáticos y de Información Electrónica.

1.- Todo usuario de Recursos Informáticos tendrá las siguientes responsabilidades:

a) Conocer y aplicar todas las medidas de Seguridad Informática emitidas por el INETER que se encuentren publicadas en la Intranet Institucional;
b) Mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario;
c) Verificar que las condiciones del lugar donde realiza sus labores sean las adecuadas para evitar que los recursos informáticos y la información bajo su resguardo puedan ser sustraídos por terceros no autorizados y en caso de no contar con las condiciones adecuadas informar a su superior inmediato, quien a su vez debe buscar una solución a su alcance o en conjunto con las áreas de apoyo o la DGSGI;
d) No mover, reubicar o llevar fuera de la institución los equipos de cómputo sin el visto bueno del responsable directo que lo tiene asignado y la debida autorización de la oficina de control de bienes;
e) Almacenar bajo llave las computadoras portátiles y dispositivos de almacenamiento removible, en gabinetes u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo, o bien asegurar con cable de bloqueo o algún otro medio que evite la sustracción no autorizada de las computadoras portátiles que se encuentren bajo su resguardo;
f) Abstenerse de instalar software sin previa justificación, notificación y autorización de la DTI;
g) Solicitar a través de la Mesa de Ayuda respectiva el apoyo para desinstalar el software del que sospeche que tiene una anomalía;
h) No modificar la configuración de hardware y software configurada por la Dirección de Infraestructura Tecnológica;
i) Reportar inmediatamente cualquier evento que pueda comprometer sus recursos informáticos tales como: virus, intrusos, modificación o pérdida de datos y otras actividades inusuales;
Apagar el equipo que tenga asignado cuando tenga que abandonar su estación de trabajo por lapsos mayores a una hora, de igual manera deberá bloquear su acceso en ausencia;

k) Utilizar la información a la que tengan acceso exclusivamente para el desempeño de su actividad profesional y laboral en la Institución;
l) Realizar respaldo de la Información Electrónica bajo su responsabilidad para la continuidad de sus funciones, cumpliendo la Normativa de Resguardo de Información No Estructurada vigente;
m) Mantener organizada su información en el disco duro local y de conservar únicamente los archivos que requiera para llevar acabo sus labores. Los archivos personales como música, fotografías, videos, juegos etc. se encuentran prohibidos y el usuario deberá hacerse responsable de los daños que causen a la información de la Institución por no acatar esta disposición; y
n) No compartir sus credenciales creadas o asignadas con ninguna persona ajena a la institución. Si por algún motivo se requiere compartir internamente, se debe notifica al superior inmediato, quien a su vez debe notificar el incidente a la DGSGI.

D.- Ambiente de Seguridad Informática del INETER.

La configuración del ambiente de Seguridad Informática del INETER estará a cargo de la DGSGI, a través de la DIT, atendiendo distintos aspectos a proteger ante las amenazas de Seguridad Informática.

1.- Seguridad en Servidores

El acceso para administración de los servidores queda restringido y únicamente para el uso de personal seleccionado de la DGSGI los cuales también podrán habilitar acceso a cuentas que administren servicios específicos de ser requerido para la operatividad de todos los procesos de la institución y los servicios que brinda.

Se prohíbe utilizar los servidores o máquinas virtuales para propósitos ajenos a la institución.

Todos los servidores o máquinas virtuales de manera indistinta al ambiente de trabajo deberán incluirse en el directorio activo de la Institución.

La actualización de los servidores Windows deberá ser gestionada a través Windows Server Updates Services para proveer de manera centralizada todas las actualizaciones de seguridad de los sistemas.

La DIT deberá realizar revisiones periódicas de actualizaciones de parches de seguridad con la finalidad de corregir vulnerabilidades presentadas por los sistemas operativos.

2.- Seguridad en Centro de Datos

Para proteger la integridad y continuidad operacional del centro de datos, este debe contar con los siguientes sistemas auxiliares de monitoreo y control:
-. Sistema de control de acceso biométrico
-. Sistema de vigilancia CCTV, para el perímetro exterior y el interior de local.
-. Sistema de climatización.
-. Sistema de generación eléctrica de respaldo.
-. Sistema de suministro eléctrico de respaldo.
-. Sistema de supresión de incendios

El acceso al centro de datos es restringido solamente al personal seleccionado de la DGSGI. Personal ajeno a la DSGI podrá ingresar con acompañamiento del personal autorizado y con previa solicitud de autorización dirigida mediante correo electrónico al Responsable de la DIT con copia al Responsable de la DGSGI o la DISUP. Se generará bitácora de accesos detallando nombre, hora de entrada y de salida, el motivo del acceso y cualquier observación oportuna.

3.- Seguridad aplicada a las Estaciones de Trabajo

a) El mantenimiento de Hardware y Software es de exclusiva responsabilidad de la Dirección General de Sistemas.
b) La DIT instalará de forma automática software de protección endpoint, el cual será el único software de este tipo autorizado para ser ejecutado en las estaciones de trabajo. El usuario deberá comunicar a la DIT los eventos o virus que fuesen detectados por su antivirus y que no hayan sido eliminados.
c) Los usuarios deberán validar el origen o contacto de correo antes de abrir o descargar archivos que a través de correo electrónico.
d) La Dirección de Infraestructura Tecnológica, realizará mantenimientos preventivos semestralmente.
e) Se documentará los cambios efectuados a nivel de configuración física y lógica sobre los equipos y cambios realizados desde su instalación.

4.- Seguridad en el Directorio Activo Institucional.

La institución debe contar con el servicio de directorio activo para facilitar la Gestión de la red de equipos de cómputo de las diferentes direcciones y áreas correspondientes, lo cual permitirá el despliegue de políticas de seguridad, instalaciones de programas y actualizaciones de sistemas. Todos los equipos deberán estar unidos al directorio.

Es responsabilidad de la Dirección de Infraestructura Tecnológica de la Información asignar un nombre de usuario único y responsabilidad del usuario contar con una contraseña robusta, las cuales deberán ser estrictamente confidenciales y no transferibles.

Se deberá implementar política de contraseña robusta para todos los servicios de TI tales como cuentas de dominio, correo electrónico y aplicaciones institucionales.

Para dar de alta o de baja una cuenta de dominio y correo electrónico se deberá dirigir un correo electrónico al responsable de la DIT con copia al responsable de la DGSGI, remitido por el Responsable de Recursos Humanos o por el Director General de la Dirección interesada, en caso de que el personal sea contratado mediante proyectos.

Adicionalmente se aplicarán políticas para denegar cambios de configuraciones en el sistema operativo a nivel de panel de control y editor de registro.

Instituto Nicaragüense de Estudios Territoriales - INETER - Dir. Gral. de Sistemas Geoinformáticos

E.- Seguridad de los Servicios Informáticos del INETER.

1.- Seguridad en Red de Datos.

Toda la red de la institución deberá encontrarse identificada por segmentos de red que específicamente agrupen a las diferentes Direcciones Generales, de igual manera cada uno de los accesos externos a la institución tales como delegaciones-barridos catastrales y estaciones de monitoreo climático, con la finalidad de aplicar restricciones de acceso a los diferentes entornos de trabajo o acceso a servicios, por tal manera todo el equipamiento de red deberá soportar la creación de VLAN's.

Se deberá habilitar o separar la red de administración de todo el equipamiento de infraestructura tecnológica el cual únicamente deberá ser accedido por la DIT.

El acceso a administración de todo el equipamiento de infraestructura tecnológica deberá realizarse únicamente a través de protocolos confiables y encriptados tales como SSH y HTTPS.

2.- Seguridad en Correo Electrónico Institucional.

Toda información de carácter laboral debe ser enviada/recibida a través de las cuentas de correo electrónico institucional. Se prohíbe el uso de cuentas personales para comunicación interna o externa

Se prohíbe el envío masivo de mensajes a través de correo electrónico, excepto en el caso de correos oficiales que podrán ser enviado por usuarios debidamente autorizados por la Dirección superior.

Cada usuario es responsable de la información que haya sido enviada a través de su cuenta.

Se prohíbe el uso del correo electrónico institucional para los siguientes motivos:

-. Utilizar el correo corporativo para mensajes de carácter personal
-. Acceder sin autorización a otra cuenta de correo electrónico
-. Transmitir mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
-. Participar en cadenas de mensajes que congestionen la red
-. Subscribirse a sitios de información no relevante que puedan ocasionar SPAM a la institución.

3.- Seguridad en el Servicio de Navegación en Internet.

Es responsabilidad del usuario hacer uso del internet únicamente con propósitos laborales, de investigación o capacitación. Queda prohibido hacer uso de algún sitio o medio no autorizado para compartir información de la Institución sin autorización o disposición de Directivos.

El usuario deberá notificar a la DIT acerca de realizar descargas que contengan un volumen de información superior a 600MB.

Instituto Nicaragüense de Estudios Territoriales – INETER – Dir. Gral. de Sistemas Geoinformáticos

Queda terminantemente prohibido el acceso a internet mediante accesos o dispositivos que no sean de la Institución tales como módems, USB o accesos inalámbricos, o redes externas al estar en el interior de la institución.

4.- Seguridad en el Acceso Remoto a la Red Local.

Se prohíbe el acceso remoto a la red Institucional a menos que sea autorizado por el Responsable de la DGSGI y Director General del área solicitante y solo a través de VPN que cuenten con las medidas de seguridad adecuadas.

5.- Seguridad en Sistemas de Información.

Todo funcionario de la DGSGI, específicamente de la DDS, o consultor de la institución deberá seguir las políticas que se detallan en a continuación, con el objetivo de proteger los sistemas de información institucionales, así como la información que a través de estos se manejan.

a) Gestión de Credenciales y accesos a los sistemas.

El acceso de los funcionarios o consultores a los sistemas de información institucionales se realizará por solicitud del Director General correspondiente, a través de correo electrónico, dirigido al Responsable de la DDS con copia al Responsable de la DGSGI. El usuario deberá de tomar responsabilidad por cada acción o transacción realizada con sus credenciales (usuario y contraseña) en los sistemas de información institucionales.

Los inconvenientes que se presenten con los sistemas de información institucionales se deberán notificar a través de la Mesa de Ayuda al Responsable de la DDS con copia al DGSGI.

b) Administración de catálogo de sistemas.

La institución deberá tener un inventario actualizado de los sistemas institucionales, ya sea desarrollado internamente o por terceros, así como la documentación técnica y de usuarios. Este inventario estará publicado a través de un catálogo virtual en la Intranet institucional.

La administración, operación y control de los sistemas de información institucionales será coordinada por el Responsable de la DDS, el Responsable de la DGSGI y según sea el caso, la Dirección General correspondiente.

c) Desarrollo de los sistemas.

Todo desarrollo de sistemas deberá cumplir con el ciclo de vida del desarrollo de software guiado por una metodología formal definida según la criticidad y prioridad del sistema a desarrollar. La DGSGI, a través de la DDS, deberá elaborar y actualizar de forma continua la Normativa de Desarrollo y Administración de Sistemas Institucionales.

Las Direcciones Generales podrán solicitar de manera formal a la DGSGI y la DDS, el desarrollo de un sistema de información o bien la actualización de sistemas lo cual deberá de estar guiado bajo la metodología definida y las debidas autorizaciones dentro de la institución.

Los procedimientos, normas, funciones y ámbito técnico de los sistemas de información deberán ser indicadas en un documento de especificaciones, el cual deberá ser debidamente aprobado por las partes involucradas. La modificación del mismo en cualquiera de las etapas del ciclo de vida deberá ser revisada, para realizar los debidos ajustes de tiempo y recursos.

Las tecnologías con las que se desarrollarán los sistemas de información deberán definirse a través de un equipo multidisciplinario conformado por la DGSGI y la DDS, especialistas, proveedores o consultores (de aplicar) y la Dirección General correspondiente.

La gestión de los accesos y credenciales utilizadas en ambientes productivos serán coordinada por el Responsable de la DGSGI.

Los sistemas de información institucionales dispondrán de tres ambientes de desarrollo separados: Desarrollo, Pruebas y Producción, los cuales deberán ser cumplidos en este orden para disponer de la versión estable en producción

d) Administración de bitácoras.

Los sistemas de información institucionales deberán implementar el uso de bitácoras, las cuales estarán clasificadas de la siguiente manera: acciones por usuarios, procesos críticos y registro de errores.

El Responsable de la DGSGI, o el Administrador de Sistemas en caso que sea un proyecto desarrollado por terceros, podrán brindar accesos a las distintas bitácoras para aquellos usuarios que estimen necesario.

e) Pruebas de los sistemas.

Las pruebas deberán ser planeadas de manera previa e indicadas en el documento de especificación correspondiente; la ejecución y resultados de estas deberán de ser debidamente documentadas, las mismas tendrán que contemplar aspectos funcionales, de seguridad y técnicos.

Los sistemas propios y los desarrollos a través de terceros deberán de contar con las pruebas en ambiente de desarrollo, prueba y documentación técnica respectiva aprobadas por las partes involucradas antes de su pase a producción.

f) Implantación de los sistemas.

Los sistemas de información realizarán su pase a producción según visto bueno de los responsables de la DDS, de la DGSGI y de la Dirección General correspondiente, esto notificado a través de correo electrónico.

Se deberá, antes de implementar los sistemas en producción, realizar la debida divulgación, capacitación y entrega de manuales de usuarios, así como verificar la completitud de toda la información técnica.

Instituto Nicaragüense de Estudios Territoriales - INETER - Dir. Gral. de Sistemas Geoinformáticos

g) Mantenimiento del Software.

Las actualizaciones de los sistemas de información en producción deberán ser autorizadas por los responsables de la DDS, de la DGSGI y de la Dirección General correspondiente.

Se deberán de seguir los puntos indicados en los acápites Desarrollo, Pruebas e Implementación y la Normativa de Desarrollo y Administración de Sistemas Institucionales.

h) Repositorio de Código Fuente.

El código fuente de los sistemas de información se resguardará en un servidor de control de código alojado en la infraestructura tecnológica de la institución. La base de datos que soporte el sistema versionador de código también debe respaldarse y resguardarse adecuadamente.

Para la creación de proyectos de equipos en el servidor de control de código, se deberá realizar la solicitud vía correo electrónica al Responsable de la DDS con copia al Responsable de la DGSGI, conteniendo la siguiente información:
-. Nombre del Proyecto.
-. Descripción del proyecto
-. Tecnologías a utilizar en el proyecto
-. Desarrolladores, los cuales deberán ser usuarios registrados en el directorio activo de la institución

Para la inclusión o eliminación de usuarios (desarrolladores) en los proyectos de equipo, se deberá realizar mediante correo electrónico al Responsable de DDS con copia al Responsable de la DGSGI.

Los desarrolladores se agregarán en los proyectos de equipos en el grupo de "Colaboradores", los miembros de este grupo pueden agregar, modificar y eliminar elementos del proyecto.

Las direcciones que realicen desarrollos a través de proyectos o consultorías deberán de asignar a un administrador de sistemas, el cual se encargará de validar que el código fuente de cada proyecto de equipo esté actualizado, sea funcional y se encuentre debidamente documentado.

El tipo de control de versiones a utilizar deberá ser elegido según las tecnologías utilizadas para el desarrollo y las necesidades propias del proyecto.

i) Adquisición de los sistemas.

La adquisición de sistemas o desarrollo a través de terceros, se deberá de gestionar por medio del Responsable de la DDS, el Responsable de la DGSI y según sea el caso, la Dirección General correspondiente.

La configuración de sistemas o desarrollos de terceros deberá realizarse por un equipo que incluyan a los proveedores, las Direcciones Generales correspondientes, la DGSGI y la DDS, dichas configuraciones deberán de contar con la aprobación correspondiente de las partes involucradas.

6.- Seguridad en servicios web y API's.

El INETER pondrá a disposición de usuarios externos y entidades, con las que se tenga convenios de integración de datos, API's y servicios web con información generada por el Instituto. Para autorizar el consumo de servicios web y API`s institucionales se deberá de realizar a través de una solicitud formal al Responsable de DDS y al Responsable de DGSGI.

El acceso a los servicios web y API´s institucionales por instituciones externas deberá realizarse a través de una configuración VPN, la cual será gestionada por el Responsable de DGSGI y el Responsable de Infraestructura Tecnológica.

Todo servicio web tanto interno o externo deberá tener configurado certificado de seguridad SSL.

Las operaciones WMS serán publicadas a través de capas, realizando peticiones en la forma de servicios y no a través de acceso del almacén de datos del servidor de mapas. Cuando sean invocadas por clientes avanzados SIG se le suministra al usuario solicitante credenciales (usuario y contraseña).

La descarga de los datos geoespaciales, mediante el servicio WFS, será restringido. En caso que sea requerido el acceso a este servicio, será con la previa autorización de la DISUP y el Responsable de la DGSGI. Con la autorización debida, la DGI otorgará el acceso a una cuenta del usuario con los permisos asignados.

Las capas que contienen información confidencial, su visualización será restringida. En caso que sea requerido el acceso a esta capa, será con la previa autorización de la DISUP y el Responsable de la DGSGI. Con la autorización debida, la DGI otorgará el acceso a una cuenta del usuario con los permisos asignados, para acceder a la información a través de los servicios WMS y WFS.

7.- Seguridad en Bases de Datos.

Para la gestión de bases de datos relacionales, la DGSGI emitirá y mantendrá actualizado Documento de Políticas de Respaldo, Resguardo y Recuperación de Bases de Datos.

En el caso de la información no estructurada, la DGSGI emitirá y mantendrá actualizado Documento de Normativa Resguardo de Información No Estructurada.

Los respaldos de las Bases de Datos e Información no Estructurada serán resguardados de manera automática en la NAS del Centro de Datos.

Los respaldos del INETER se almacenarán en cintas magnéticas, dichos respaldos deberán realizarse diariamente de manera automática, y se garantizan los respaldos Completos e Incrementales, los cuales se entregarán al Responsable de la DGSGI.

La DGI es la encargada de monitorear el funcionamiento de los recursos de los servidores de bases de datos.

La DGI es la encargada de enviar alertas y notificaciones de los servidores con administración compartida a los Administradores de Bases de Datos y a la DDS, en caso que se presente un comportamiento inusual.

VI.- Interpretación

La interpretación de las presentes políticas, para efectos administrativos, corresponde a la DGSGI, quien también resolverá los casos no previstos por las mismas.

Transitorios

1. Las presentes Políticas entrarán en vigor a partir de la publicación de la respectiva Resolución Administrativa.
2. El presente documento fue emitido por la DGSGI del Instituto Nicaragüense de Estudios Territoriales el 31 de julio de 2011.

Última hoja de las Políticas de Seguridad Informática para el INETER emitidas por la DGSGI el día 31 de julio de 2020 y publicadas en la Intranet Institucional el día 6 del mes de agosto de 2020, mismas que hacen constar de 18 hojas útiles.

Luis Manuel Herrera Ordóñez
Asesor Técnico de Sistemas Geoinformáticos

Wesley Guillermo Sang Fuentes
Dir. de Infraestructura Tecnológica

Instituto Nicaragüense de Estudios Territoriales - INETER - Dir. Gral. de Sistemas Geoinformáticos

Meyling Fabiola Castillo
Dir. de Desarrollo de Software Geoinformático

Meyling Izayana Sierra Mejía
Dir. de Georepositorio Institucional