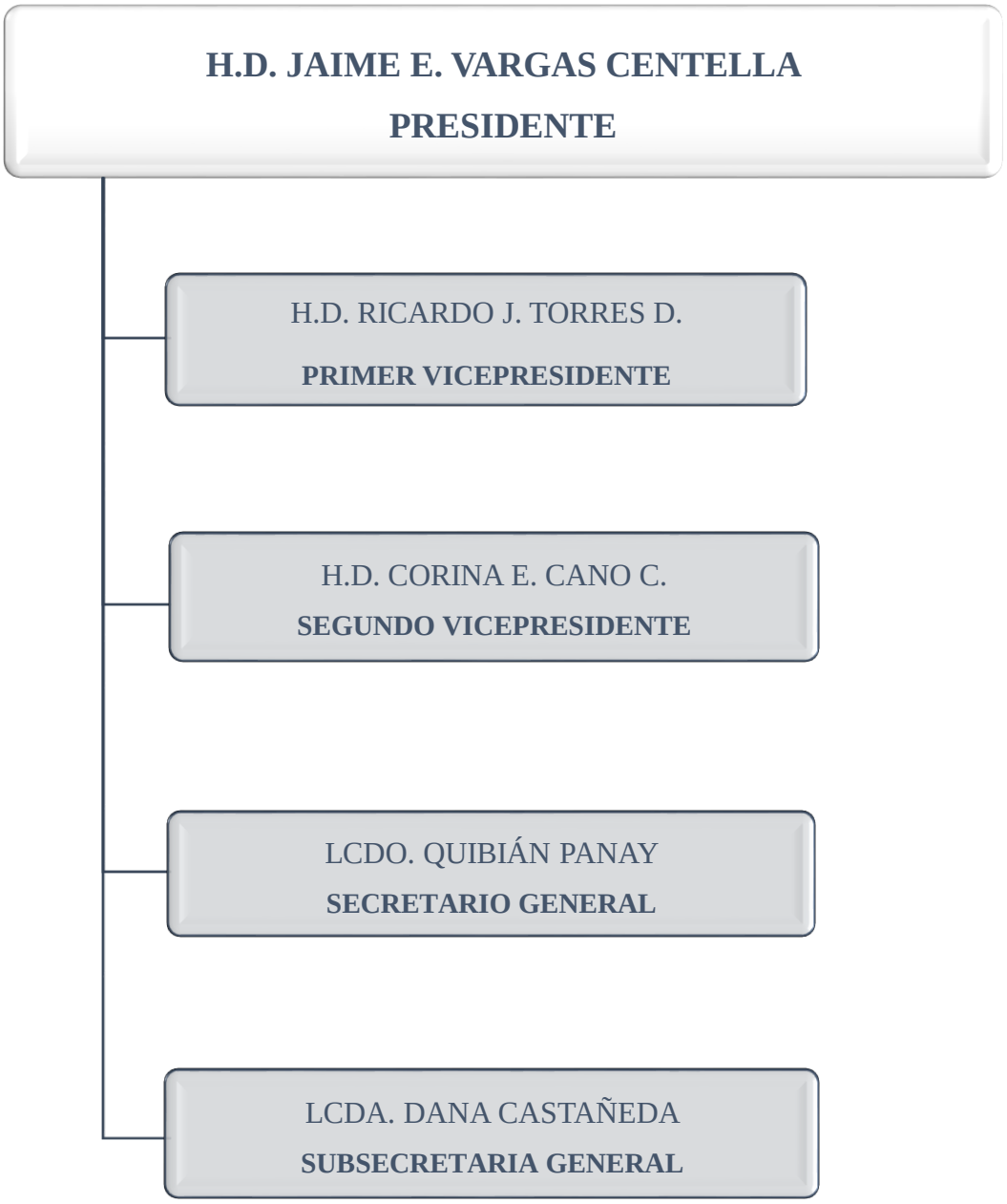
MANUAL DE PROCEDIMIENTOS ADMINISTRATIVOS

UNIDAD DE SEGURIDAD INFORMÁTICA

AN_USI_15_JUL_2023

VERSIÓN 1

DIRECTIVA DE LA ASAMBLEA NACIONAL



SECRETARÍA GENERAL

DIRECCIÓN DE DESARROLLO INSTITUCIONAL

LCDA. LUZ MARINA NAVARRO GUTIÉRREZ
DIRECTORA

PERSONAL TÉCNICO

BERTA HISLOP	ANALISTA
MARKELDA CAÑIZALES	ANALISTA
MELINA OROCU	ANALISTA
YERITZA CASTILLERO	ASISTENTE DE ANALISTA
GLORIA GIL	ASISTENTE ADMINISTRATIVA
MATILDE BUSTAMANTE	SECRETARIA

UNIDAD DE SEGURIDAD INFORMÁTICA

ING. NAYUBEL RUIZ

DEPARTAMENTO DE REVISIÓN Y CORRECCIÓN DE ESTILO

DIANA RODRÍGUEZ
CORRECTORA

ÍNDICE

INTRODUCCIÓN

La Asamblea Nacional en su constante proceso de modernización cuenta hoy día con herramientas tecnológicas que permiten el acceso oportuno a la información y la rápida comunicación con el mundo.

Esta plataforma tecnológica hace posible que los colaboradores de la institución realicen sus tareas de forma eficiente y a la vez brinda a la población la oportunidad de mantenerse actualizada de toda la gestión legislativa.

Las computadoras, los servidores y las redes son instrumentos que permiten de forma eficiente el acceso y distribución de la información, por lo que se consideran una infraestructura estratégica para el desarrollo de los objetivos de la organización.

El presente Manual de Procedimientos es una herramienta que permite conocer los pasos que deben ejecutarse para mantener de forma segura la estructura tecnológica en la Asamblea Nacional, al mismo tiempo busca establecer una cultura de calidad operada de forma confiable, siendo la seguridad informática, el medio donde se valoran y administran los riesgos apoyados en estrategias y estándares que cubren las necesidades en materia de seguridad.

El desarrollo de este manual, además, tiene como finalidad estructurar los criterios de seguridad de la información sistematizada en la institución, establecer un control de usuarios de la red y plasmar lineamientos en esta materia.

Las políticas de seguridad informática establecidas en este manual son la base fundamental para la protección de los activos informáticos y de toda la información que se esgrime en el Parlamento.

Este documento debe ser renovado en la medida en que se realicen cambios y se incorporen nuevos procesos en dicha unidad, con el propósito de conservar este material siempre actualizado.

El precitado manual está integrado por el marco jurídico que fundamenta los procedimientos, los objetivos, las normas de operación, la descripción narrativa, los diagramas de flujo y los formatos e instructivos de llenado.

De acuerdo con la política de calidad de la Asamblea Nacional el manual debe ser renovado cada tres años o en la medida en que se realicen cambios legales, así como en la forma de realizar las diferentes actividades que motiven la incorporación de nuevos procesos en dicha unidad, con el propósito de conservar este material siempre actualizado.

I

• GENERALIDADES

I. GENERALIDADES

El presente manual contiene los lineamientos y procedimientos que tienen por objeto establecer medidas y patrones técnicos de administración y organización de las tecnologías de información y comunicación de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la institución.

También se convierte en una herramienta de trabajo que muestra las políticas de seguridad informática al personal de la unidad, facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada, así como el manejo de datos y el uso de bienes informáticos, tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información.

I.1. Política de calidad

La Asamblea Nacional ejerce la función legislativa del Estado panameño que consiste en la elaboración de proyectos de ley; dirige sus esfuerzos para mantener la política de puertas abiertas, contribuyendo a la satisfacción de las necesidades de nuestras partes interesadas en los diferentes sectores de la vida ciudadana, manteniendo la transparencia, la igualdad, la ética, la justicia, la sensatez, el balance de poderes para las transformaciones sociales. Esto lo lograremos cumpliendo con los requisitos legales, personal competente y la mejora continua en nuestros procesos.

I.2. Objetivos de calidad

Nuestros objetivos están enfocados en el cumplimiento de la política de calidad y los requisitos de nuestros usuarios, por lo que buscamos la mejora continua de nuestros procesos encaminados a:

- Fortalecer las competencias laborales.
- Cumplir con los tiempos de respuesta a los usuarios.
- Lograr el grado de satisfacción del cliente.
- Promover la mejora continua del Sistema de Gestión de Calidad.

I.3. Objetivo general

Propender que los servicios de seguridad tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad óptimo y que permitan:

• Disminuir las amenazas a la seguridad de la información y los datos.

• Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.

• Cuidar y proteger los recursos tecnológicos de la Asamblea Nacional.

• Concientizar a los funcionarios sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

I.4. Objetivos específicos

El Manual de Procedimientos de la Unidad de Seguridad Informática es un instrumento técnico de automatización que tiene los siguientes objetivos:

1.1.1 Establecer formalmente los procesos requeridos para la ejecución de las tareas y lograr el cumplimiento de los objetivos funcionales y estratégicos de la Unidad de Seguridad Informática.

1.1.2 Ser utilizado como instrumento de información y medio de capacitación para alinear persistentemente al personal.

1.1.3 Instaurar las bases para mantener un firme sistema de control interno que facilite el proceso de las tareas encomendadas.

I.5. Ámbito de aplicación y alcance del manual

El Manual de Procedimiento Administrativo de la Unidad de Seguridad Informática es de fiel cumplimiento para todas aquellas unidades y funcionarios que intervienen en el proceso.

I.6. Responsabilidad

El jefe de la Unidad de Seguridad Informática deberá poseer un ejemplar completo de este manual con el deber de observar y supervisar el cumplimiento de las normas específicas y procedimientos contenidos en él.

Los funcionarios son responsables ante su jefe superior a quien deberán notificar cualquier irregularidad, inconformidad, desacuerdo o sugerencia con lo descrito en los procesos y procedimientos a fin de mejorarlos.

Todos los colaboradores de la Asamblea Nacional tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de tecnología bajo su control, de acuerdo con las instrucciones y la capacitación recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y deben discriminarse dichas responsabilidades de aquellas que sean incompatibles cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

Todos los colaboradores de la Asamblea Nacional son responsables de:

a) cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;

b) mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;

c) proteger la seguridad de los equipos de cómputo, así como de la información bajo su control directo;

d) informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de esta, incluyendo sospechas de divulgación de contraseñas, y

e) acatar todos los lineamientos establecidos dentro de este documento.

I.7. Estructura de códigos de los procedimientos administrativos y sus formatos

Para la adecuada identificación y control de los procedimientos que se desarrollan en las distintas unidades administrativas de la Asamblea Nacional, se ha considerado la introducción de una codificación única en sus procedimientos y formatos.

Esta codificación digital se hará de la siguiente manera: A todos los procedimientos y formatos que utilicen las unidades administrativas se les asignará un número, las siglas de la Asamblea Nacional, el respectivo nombre de la dirección, del departamento o sección, según sea el caso.

Unidad de Seguridad Informática	
Código para Manual de Procedimiento	AN_SG_USI_DIA_MES_AÑO
	Versión 0
	Fecha: día_mes_año
Código para Procedimientos	AN_SG_USI_P.A.01
	Versión 0
	Fecha: día_mes_año
Código para formularios	AN_SG_USI_01
	Versión 0
	Fecha: día_mes_año

Este manual es entregado a la Unidad de Seguridad Informática y, posteriormente, será publicado en la página web de la institución. Los formularios, formas y documentos en este manual están codificados. Estos formularios, formas y documentos podrán ser modificados, cambiados y sustituidos.

Para realizar dicho cambio se deberá enviar una nota a la Dirección de Desarrollo Institucional, previo aviso, y de esta forma se realizarán los cambios necesarios. Para buscar el manual de la unidad deberán acceder al sitio web https://asamblea.gob.pa/transparencias, renglón de transparencia, artículo 9.4 Manuales de Procedimientos.

II

• BASE LEGAL

II. BASE LEGAL

-**Constitución Política de la República de Panamá de 1972**, reformada por los Actos Reformatorios de 1978, por el Acto Constitucional de 1983, los Actos Legislativos 1 de 1993 y 2 de 1994 y por el Acto Legislativo N°1 de 2004.

-**Reglamento Orgánico del Régimen Interno de la Asamblea Nacional** que integra la Ley 49 de 4 de diciembre de 1984, que lo adoptó originalmente, con las modificaciones, adiciones y derogaciones aprobadas por la Ley 7 de 1992, la Ley 3 de 1995, la Ley 39 de 1996, la Ley 12 de 1998, la Ley 16 de 1998, la Ley 35 de 1999, la Ley 57 de 2002, la Ley 25 de 2006, la Ley 16 de 2008, la Ley 28 de 24 de febrero de 2010, la Ley 28 de 2009, la Ley 32 de 2009, la Ley 38 de 2009, la Ley 43 de 2009 y la Ley 66 de 2009, sobre la base del Texto Único publicado en la Gaceta Oficial No. 26476- D de 24 de febrero de 2010.

-**Ley 6 de 22 de enero de 2002**, que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones. (Gaceta Oficial No. 24.476 de 23 de enero de 2002).

-**Ley 65 de 30 de octubre de 2009,** establece que la Autoridad Nacional para la Innovación Gubernamental es la autoridad competente del Estado para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las TIC en el sector gubernamental para la modernización de la gestión pública, así como recomendar la adopción de políticas, planes, acciones estratégicas nacionales relativas a esta materia.

-**Ley 39 de 30 de mayo de 2017,** que modifica y adiciona artículos a la Ley 12 de 1998, que desarrolla la Carrera del Servicio Legislativo y dicta otras disposiciones.

-**Resolución 42 de 9 de junio de 1998 de la Directiva de la Asamblea Legislativa**, por la cual se aprueba la nueva estructura administrativa del Órgano Legislativo.

-**Resolución 72 de 11 de julio de 2000**, por la cual se modifica la estructura administrativa del Órgano Legislativo.

-**Resolución 80 de 9 de agosto de 2001**, por la cual se modifica la estructura organizativa de la Asamblea Legislativa.

-Resolución 263 de 30 de junio de 2008, por la cual se crea la Unidad de Seguridad Informática, integrada al nivel coordinador, posteriormente bajo la **Resolución 52 de 12 de agosto de 2009**, se modifica la estructura organizativa y pasa a formar parte de la Dirección de Tecnología, Informática y Comunicaciones y, posteriormente, mediante la **Resolución 47 de 5 de agosto de 2010**, se extrae de la Dirección antes mencionada para ser integrada el nivel fiscalizador bajo el nombre de Unidad de Seguridad Informática.

-Resolución 145 de 12 de enero de 2023, por la cual se aprueba el cambio de denominación de la Dirección de Estudios Parlamentarios y Red Global de Información Legal (GLlN) a Dirección de Estudios Parlamentarios; se elimina la Oficina de Asesoría y Red Global de Información Legal (GLIN) y se crea la Oficina de Análisis y Seguimiento de Convenios de la Dirección de Estudios Parlamentarios y se crea el Departamento de Responsabilidad Social y Sostenibilidad Institucional adscrito a la Dirección de Recursos Humanos de la estructura organizativa de la Asamblea Nacional.

III

• CONCEPTOS Y DEFINICIONES

III. CONCEPTOS Y DEFINICIONES

1. **Organigrama**

   Representación gráfica de la estructura de una empresa o una institución, en la cual se muestran las relaciones entre sus diferentes partes y la función de cada una de ellas, así como de las personas que trabajan en estas.

2. **Firma de autorización**

   Firma de la persona que tiene la autoridad para determinar la responsabilidad de cada área en la elaboración, revisión y autorización de documento.

3. **Software**

   Conjunto de programas de distintos tipos (sistema operativo y aplicaciones diversas) que hacen posible operar con el ordenador.

4. **Hardware**

   Componentes físicos de un computador y sus periféricos.

5. **Stock**

   Cantidad de productos, materias primas, herramientas, etc., que necesitan ser almacenadas para compensar la diferencia entre el flujo del consumo y el de la producción.

6. **Datos**

   Información concreta sobre hechos, elementos, etc., que permite estudiarlos, analizarlos o conocerlos.

7. **Correo electrónico**

   Un correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante redes de comunicación electrónica.

8. **Usuario de red**

   En informática y la cultura web, se entiende por **usuario** a un conjunto de permisos y de recursos asignados a un operador como parte de una **red** informática, y que bien puede ser una persona, un programa informático o un computador.

9. **Red compartida**

   Es un conjunto de equipos, nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

10. **Sistema**

    Un sistema operativo es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.

11. **Dominio**

    Dominio de internet es un nombre único que identifica a una sub área de internet.

12. **Estrategia**

    Diseñar la estrategia tecnológica que deberá tomar en cuenta el potencial de las TI.

13. **Desempeño**

    Las TI deberán proporcionar el soporte a la Asamblea Nacional, ofreciendo servicios con los niveles y la calidad requeridos.

14. **Sistema Operativo**

    Programa o conjunto de programas que actúan como intermediarios entre las aplicaciones de los usuarios (Software) y el equipo físico (Hardware) de la máquina, ocultando las características particulares de este último.

15. **Aplicaciones**

    Nombre que reciben los programas especializados en tareas concretas y de una cierta complejidad.

16. **Bases de Datos**

    Es la colección de información que está organizada de forma tal que su contenido sea fácilmente accedido, administrado y actualizado.

17. **Respaldo**

    Sinónimo de backup.

18. Backup

Copia idéntica de algo, copia de seguridad o copia respaldo de algo.

19. Confidencialidad

Aseguramiento de que la información es accedida solo por el personal autorizado.

20. Integridad

Garantía de la exactitud y completitud de la información y los métodos de procesamiento.

21. 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.

22. Usuario

Es la persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional.

23. Políticas de seguridad

Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de esta.

24. Password

Es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador o a un programa.

25. Sistema de información

Es un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.

26. Mensajería Instantánea (conocida también en inglés como IM).

Es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red como Internet.

27. FTP (Protocolo de Transferencia de Archivos)

Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

28. Servidor Web

Es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o aplicación del lado del cliente.

29. RDSI

Es una red que procede por evolución de la Red Telefónica Básica (RTB) o Red Telefónica Conmutada (RTC) convencional, que facilita conexiones digitales de extremo a extremo entre los terminales conectados a ella (teléfono, fax, ordenador, etc.).

30. ADSL

Es una tecnología de acceso a internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa.

31. Routers

Es un dispositivo de hardware que permite la interconexión de ordenadores en red.

32. Módem

Es un dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (desmodulación), y permite así la comunicación entre computadoras a través de la línea telefónica o del cable módem.

33. Redes

Conjunto de equipos informáticos conectados mediante dispositivos físicos de transporte de datos.

34. Freeware

Se refiere a aplicaciones o software de ordenador gratis.

35. Open Sourse (Código abierto)

Es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales, las cuales destacan en el llamado software libre.

36. Cookies

Pequeña información enviada por un sitio web y es almacenada en el navegador del usuario.

37. Auditoría externa

Es un examen crítico, objetivo, sistemático y detallado de un sistema de información informático.

38. Auditoría interna

Ayuda a cumplir los objetivos de la institución aportando un enfoque sistemático y disciplinado que permite evaluar y mejorar la eficacia de los procesos de gestión de los riesgos informáticos y su respectivo control.

39. Incidente

Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información. Un impedimento en la operación normal de las redes, sistemas o recursos informáticos o cualquier acto que implique una violación a la política de la seguridad informática de la institución.

40. Riesgo

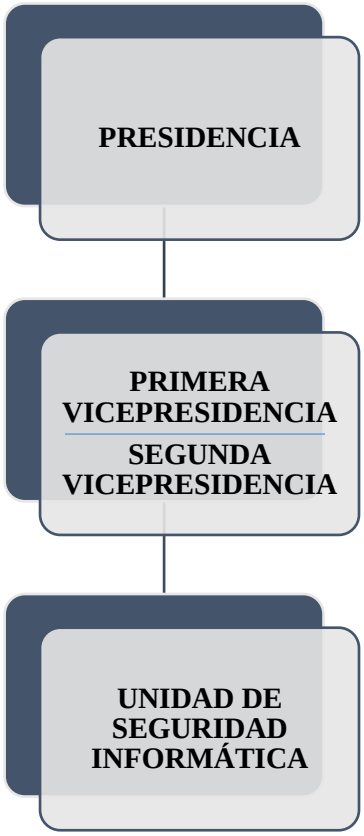
Es una medida de la magnitud de los daños frente a una situación peligrosa. Ocurrencia potencial de perjuicio o daño para cualquier recurso informático.

IV

• ESTRUCTURA ORGANIZATIVA

IV. ESTRUCTURA ORGANIZATIVA

Organigrama



V

• FUNCIONES GENERALES

V. FUNCIONES GENERALES

Objetivo

Asegurar que se cumplan las políticas de seguridad, normas y procedimientos de acceso y utilización de los sistemas de informática en la Asamblea Nacional.

Funciones:

– Diseñar políticas para la implementación, administración y uso seguro de los sistemas de informática y comunicaciones que se administren a nivel institucional.
– Contribuir al desarrollo del modelo de aseguramiento de la calidad de los sistemas y servicios informáticos que provee la Dirección de Tecnología Informática y Comunicaciones.
– Promover el cumplimiento de las normas de seguridad para el acceso a los sistemas de informática y comunicaciones instalados en la institución.
– Garantizar los planes de seguridad para minimizar la vulnerabilidad de los sistemas de informática institucional y para asegurar la recuperación de las operaciones de cómputo ante fallas menores y/o mayores.
– Evaluar periódicamente las políticas y normas de seguridad informática, adecuándolas a los riesgos y vulnerabilidades vigentes.
– Elaborar el plan anual de trabajo de sus actividades y proyectos.
– Confeccionar los informes de seguimiento sobre la ejecución de sus labores.
– Elaborar los informes de evaluación de resultados.
– Formular el anteproyecto de presupuesto de la unidad.
– Ejercer las demás funciones que se le asignen afines a su área de especialidad.

VI. LINEAMIENTOS DEL MANUAL DE SEGURIDAD INFORMÁTICA

VI.1. CLASIFICACIÓN DE LA INFORMACIÓN

- **Información de acceso libre.**

Todo tipo de información en manos de agentes del Estado o de cualquiera institución pública que no tenga restricción.

- **Información de acceso restringido.**

Todo tipo de información en manos de agentes del Estado o cualquier institución pública, cuya divulgación haya sido circunscrita únicamente a los funcionarios que la deban conocer en razón de sus atribuciones y de acuerdo con la ley.

- **Información confidencial.**

Todo tipo de información en manos de agentes del Estado o de cualquier institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, u orientación sexual, su historial penal y policivo, correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. Para efectos de la ley, también se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios.

VI.2. POLÍTICA

1. Sobre la integridad y disponibilidad de los recursos

Los usuarios deben respetar la integridad de los recursos y sistemas de información. Para ello se enumeran una serie de regulaciones a saber:

1.1. Un usuario no debe alterar o eliminar ordenadores (hardware o configuración de SO), software o periférico que estén asignados a este u otro usuarios.

1.2. Los usuarios no deben entorpecer o absorber recursos compartidos de forma tal que impidan a otros realizar tareas de una forma eficiente. Esto incluye lo siguiente:

1.2.1. El envío a través de correo electrónico de cartas encadenadas o mensajes excesivamente voluminosos o con muchos destinatarios, ya sean locales o ajenos a la institución.

1.2.2. Uso de programas que puedan saturar los servidores o las redes de la Asamblea Nacional, cuando haya alternativas más eficientes o no tengan una prioridad alta. En cualquier caso, se deberá solicitar con la suficiente antelación al responsable informático.

1.2.3. Modificación no autorizada de privilegios o permisos.

1.2.4. Intentos de desactivar servidores o cortar el funcionamiento de las redes.

1.2.5. Intento de realizar cualquier tipo de daño (físico o lógico) a las herramientas informáticas (equipos, aplicaciones, documentos, entre otros) de la Asamblea Nacional.

Los usuarios no deben, intencionadamente, desarrollar o usar programas cuyo objetivo sea dañar otras máquinas o acceder a recursos restringidos (malware, virus, troyanos, puertas traseras, otros). Más aún, deben controlar que no se les infecte su equipo con este tipo de software, para lo cual la Dirección de Tecnología con la Unidad de Seguridad Informática, deben proporcionar las herramientas y utilidades adecuadas. El uso de este tipo de programas, contra un agente externo o contra la propia Asamblea Nacional, pueda incluso, implicar acciones legales por la parte afectada.

1.3. El usuario a quien se le asigne un equipo de tecnología es responsable de este y debe informar inmediatamente si el equipo es robado, dañado y, en general, si por cualquier causa resulta inutilizable. Para efectos de implementar los reportes de daños, el usuario debe llamar, a la brevedad posible, a la Dirección de Tecnología a la extensión especial Nº 8000.

1.4. El usuario a quien se le asigne un equipo de tecnología móvil estará autorizado para movilizar el equipo fuera de la institución, siempre que sea necesario, por medio de la nota de asignación del equipo por parte de la autoridad correspondiente (Secretaría General, Dirección General de Administración y Finanzas y/o Dirección de Tecnología de Informática y Comunicaciones). La autorización estará vigente mientras el usuario sea funcionario de la Asamblea Nacional, hasta que las autoridades correspondientes tengan a bien suspender la orden, o en caso de que se asigne un equipo no móvil en su reemplazo.

1.5. Ninguna computadora o equipo de telefonía fijo o móvil podrá ser reparado por los usuarios. En caso de presentarse algún daño en los equipos, se debe notificar inmediatamente al escritorio de ayuda de la Dirección de Tecnología para que sea revisado, y si la garantía estuviese vigente, hacerla efectiva ante el correspondiente proveedor.

1.6. Los usuarios de las redes no deben utilizar los enlaces de red para otros usos que no sean los permitidos o los necesarios para el buen desempeño de sus actividades.

2. Accesos no autorizados y suplantación de identidad

2.1. Los usuarios no deben tratar de conseguir accesos a sistemas o recursos no autorizados ni permitir o facilitar que otros lo hagan.

2.2. Los usuarios deben respetar los derechos del resto de usuarios. La mayoría de los sistemas de uso compartidos proporcionan mecanismos para proteger los datos e información privada de posibles consultas de otros. Los intentos de saltarse estos mecanismos para conseguir accesos no autorizados a información calificada como personal, supondrán una violación de esta política.

2.3. Los administradores de sistemas que estén autorizados podrán acceder, exclusivamente, por motivos de mantenimiento y/o seguridad, a aquellas carpetas de usuario que permitan al administrador detectar, analizar y seguir las pistas de una determinada sesión o conexión.

2.4. En cualquier caso, el administrador de sistemas tiene el deber de guardar secreto el contenido de las carpetas de los usuarios, no estando autorizado a permitir que terceros puedan acceder a esta información.

2.5. En el supuesto de que una política interna expresamente lo autorice, el administrador de sistemas podrá permitir el acceso a terceros (responsables de proyectos, directores, jefes) a determinadas carpetas de otros usuarios, debiendo contar en todo caso, tanto con la autorización del secretario general de la Asamblea Nacional y con el propietario de la carpeta.

2.6. Los usuarios de los recursos informáticos de la Asamblea Nacional no deben acceder a ordenadores, aplicaciones, datos, información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir, de forma intencionada, que

otros lo hagan, independientemente de que el recurso (equipo, aplicación, red, datos, otros) pertenezca o no a la Asamblea Nacional.

2.7. No está permitido realizar, de forma malintencionada, acciones cuyo fin sea la obtención de contraseñas de otros usuarios sin el consentimiento de estos.

2.8. Cualquier defecto o anomalía que se descubra en el sistema o en su seguridad se debe reportar, con la mayor brevedad posible, a la Unidad de Seguridad Informática y/o Dirección de Tecnología Informática y Telecomunicaciones. La Unidad de Seguridad Informática estará encargada de investigar y proponer soluciones al problema.

2.9. Todo aquel usuario que haya sido autorizado a utilizar una cuenta mediante un sistema de login/password será responsable de mantenerla en secreto y no darla a nadie sin la autorización del administrador del sistema (DITIC) y la (USI), además de ser siempre el responsable de lo que se ejecute en el sistema desde esa cuenta.

2.10. Los usuarios deben evitar tener recursos compartidos (carpetas, directorios, entre otros) sin los mecanismos de aplicación que garanticen la seguridad de su equipo y la red, y la seguridad necesaria y disponible en cada sistema operativo y/o sin la autorización del administrador del sistema.

3. Uso de los servicios de comunicación y difusión de información

El correo electrónico, las listas de distribución y servicios de mensajería instantánea son herramientas que facilitan la comunicación entre personas. Por ello, conviene tener en cuenta una serie de comportamientos a la hora de usar estos medios.

3.1. No se deben usar estas utilidades para el envío de mensajes de contenido fraudulento, ofensivo, obsceno o amenazante.

3.2. Las listas de distribución de correo se deben usar solo para enviar mensajes relacionados con las funciones que desempeñan los usuarios en la institución.

3.3. Los recursos de la Asamblea Nacional no se deben usar para actividades personales que no tengan relación con las propias del desempeño laboral. En este caso el responsable informático no está obligado a prestar soporte.

3.4. No se deben usar estos servicios con fines comerciales.

4. Uso de la infraestructura de comunicaciones

4.1. Es prohibido instalar servicio telemático (correo electrónico, servidores web, FTP, otros) sin la autorización expresa del responsable administrativo con la designación de un administrador del sistema (DITIC) y de la Unidad de Seguridad Informática.

4.2. No se puede realizar conexión, desconexión o reubicación de equipos o cambios de configuración de estos mismos sin la autorización expresa de responsable administrativo (director) y del administrador del sistema (DITIC), notificando Unidad de Seguridad Informática.

4.3. Es prohibido la instalación de dispositivos, tarjetas de accesos remoto, módems, RDSI, ADSL, routers o cualquier otro dispositivo de comunicaciones en ordenadores o redes sin la autorización expresa del responsable administrativo, del administrador del sistema (DITIC) y la Unidad de Seguridad Informática.

4.4. Es prohibido la conexión de equipos de comunicación para intercambio de información (rutas, redes, otros) entre ordenadores de las redes de la Asamblea Nacional y otros ajenos a dichas redes.

4.5. Es prohibido el uso de la red y ordenadores de la Asamblea Nacional para conseguir acceso no autorizado a cualquier ordenador.

4.6. Es prohibido instalar o ejecutar en cualquier punto de la red informática (ordenadores o software de red) programas o carpetas que traten de descubrir información distinta de los propios usuarios, en cualquier elemento de la red. Esto incluye sniffer, escaneadores de puertos, entre otros.

4.7. No se debe facilitar a una tercera entidad acceso, a través de las redes de la Asamblea Nacional, a la infraestructura de comunicaciones propias de este organismo; es decir, no se puede proporcionar tránsito a terceras instituciones, salvo obtención del consentimiento, previamente solicitado, de la Secretaría General de la Asamblea Nacional, en su calidad de responsable administrativo de los recursos informáticos de la Asamblea Nacional.

4.8. Se debe evitar la circulación de información comercial, con excepción de respuestas a peticiones expresas de información sobre producto o servicios de interés para las actividades habituales del organismo.

4.9. No proceder a la destrucción, manipulación o apropiación indebida de la información que circule por la red.

4.10. Evitar el consumo excesivo de los recursos por parte de cualquier usuario.

4.11. Respetar el derecho de privacidad de los diferentes usuarios de la red.

4.12. La infraestructura de red de la Asamblea Nacional nunca deberá ser utilizado, bajo ningún concepto, para lo siguiente:

- Transmisión de información o acto que viole la legislación vigente de la República de Panamá.
- Fines privados o personales, con o sin ánimo de lucro.
- Fines relativos a juegos.
- Fines no estrictamente relacionados con las actividades propias del Organismo.
- Creación o transmisión de cualquier tipo de información que sea ofensiva, obscena o indecente.
- Transmitir información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- No divulgar información que viole los derechos de propiedad intelectual.
- No usar cualquier aplicación de la cual se sepa que su uso pueda suponer una alteración de la red.

5. Licencias de Software y derechos de autor

Los usuarios y administradores deben respetar las condiciones de licencia y derecho de autor del software que usen en sus equipos.

5.1. Todo software adquirido para la Asamblea Nacional (licencias para estaciones de trabajo o licencias para instalación en servidores centrales) debe estar debidamente licenciado, y la responsabilidad de esto recaerá en el director general de

Administración y Finanzas, el director de Tecnología Informática y Comunicaciones, y el responsable del servicio que haya autorizado su adquisición.

5.2. Todo software que se use en la Asamblea Nacional para fines administrativos debe estar debidamente licenciado, con un número de licencia que corresponda con el número de usuario simultáneo. Podrá usarse en equipos de la Asamblea Nacional software "libre" (OpenSource, freeware, otros) siempre y cuando cuente con la autorización de la Dirección de Tecnología Informática y Comunicaciones, además de la verificación de la Unidad de Seguridad Informática.

5.3. Todo software que se use y esté protegido por derecho de autor no puede ser copiado, salvo con autorización del propietario. No se podrán usar los medios que la Asamblea Nacional pone a disposición de sus funcionarios para copiar softwares protegidos o romper con las medidas de protección de estos.

5.4 Aparte del software, toda información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo o red, se debe usar de acuerdo con la legislación vigente.

5.5. Los usuarios responderán siempre, personalmente, por el software que esté instalado en sus equipos, así como del uso que se efectúe, y deberán cumplir con las obligaciones y requisitos que se derivan de su instalación y utilización.

Los usuarios no podrán permitir, en ningún caso, que una persona lleve a cabo la instalación en sus equipos de softwares que no estén debidamente licenciados.

El incumplimiento de estas obligaciones por parte de los usuarios dará lugar a la aplicación de las medidas preventivas, correctivas y disciplinarias previstas en el Cuadro de Sanciones y, en su caso, al ejercicio de las acciones legales pertinentes.

6. Adquisición de tecnología

La tecnología, además de múltiples beneficios también, trae consigo riesgos por tal razón, debemos velar para que tecnología que vayamos a adquirir no represente amenaza alguna y tomar las medidas pertinentes para su disminución o erradicación.

La adquisición de tecnología debe ser coordinada con los expertos, con el fin de que sea adaptable a las ya existentes y asegurar su desempeño óptimo.

6.1. Toda adquisición de tecnología debe ser coordinada con la Secretaría General y la Dirección de Tecnología.

6.2. La compra de tecnología debe contemplar las medidas de seguridad pertinentes recomendadas por la Unidad de Seguridad Informática.

En cualquier caso, es responsabilidad de los directores, jefes de departamentos o personas designadas por estos, dar la difusión necesaria de estas normas para que sean conocidas por todos los agentes a los que se les aplica.

VI.3. CONSECUENCIAS DEL MAL USO DE LOS RECURSOS TECNOLOGÓGICOS

1. Colaboración de los usuarios

Los usuarios, cuando se les solicite, debe colaborar con los administradores del sistema (DITIC) y la Unidad de Seguridad Informática, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.

2. Acciones correctivas y preventivas

Si los administradores del sistema (DITIC) y la Unidad de Seguridad Informática general o local, detectan la existencia de un mal uso de los recursos y este procede de las actividades o equipo de un usuario determinado, pueden tomar cualquiera de las siguientes medidas para proteger a los otros usuarios, redes o equipos:

- Notificar la incidencia al usuario o responsable del sistema.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.
- Con el permiso del responsable de seguridad y la debida justificación, inspeccionar carpetas o dispositivos de almacenamiento del usuario implicado.
- Informar a los superiores correspondientes de lo sucedido.
- Toda aplicación de medidas disciplinarias se tomará de acuerdo con lo establecido en el Reglamento de Administración de Recursos Humanos y Cuadro de Aplicaciones.

VI

• PROCEDIMIENTOS Y FLUJOGRAMAS

ASAMBLEA NACIONAL
SECRETARÍA GENERAL
DIRECCIÓN DE DESARROLLO INSTITUCIONAL

NOMBRE DEL PROCEDIMIENTO
RESTRICCIÓN DE EQUIPO POR AMENAZA O MAL USO DEL INTERNET

VERSIÓN DEL PROCEDIMIENTO No. 1

CÓDIGO
AN_SG_USI_P.A.01

FECHA
15 DE JULIO DE 2023

VALIDADO POR
Ing. Nayubel Ruiz-Jefe
Unidad de Seguridad Informática

DOCUMENTADO POR
Mgtr. Markelda Cañizales-Analista
Dirección de Desarrollo Institucional

DESCRIPCIÓN DEL PROCEDIMIENTO
OBJETIVO:
Identificar y administrar de forma continua los equipos informáticos a efecto de reducir los riesgos a los que se encuentra expuesto constantemente.

Unidades administrativas y funcionarios que intervienen en el proceso

Paso	Responsable	Descripción del procedimiento	Formulario
1	Unidad de Seguridad Informática	-Detecta el uso irregular del internet por medio del sistema automatizado vigente utilizado por la unidad. -Envía alerta al correo electrónico de la unidad de seguridad informática. Nota: El sistema de monitoreo suministra como mínimo:	Correo electrónico

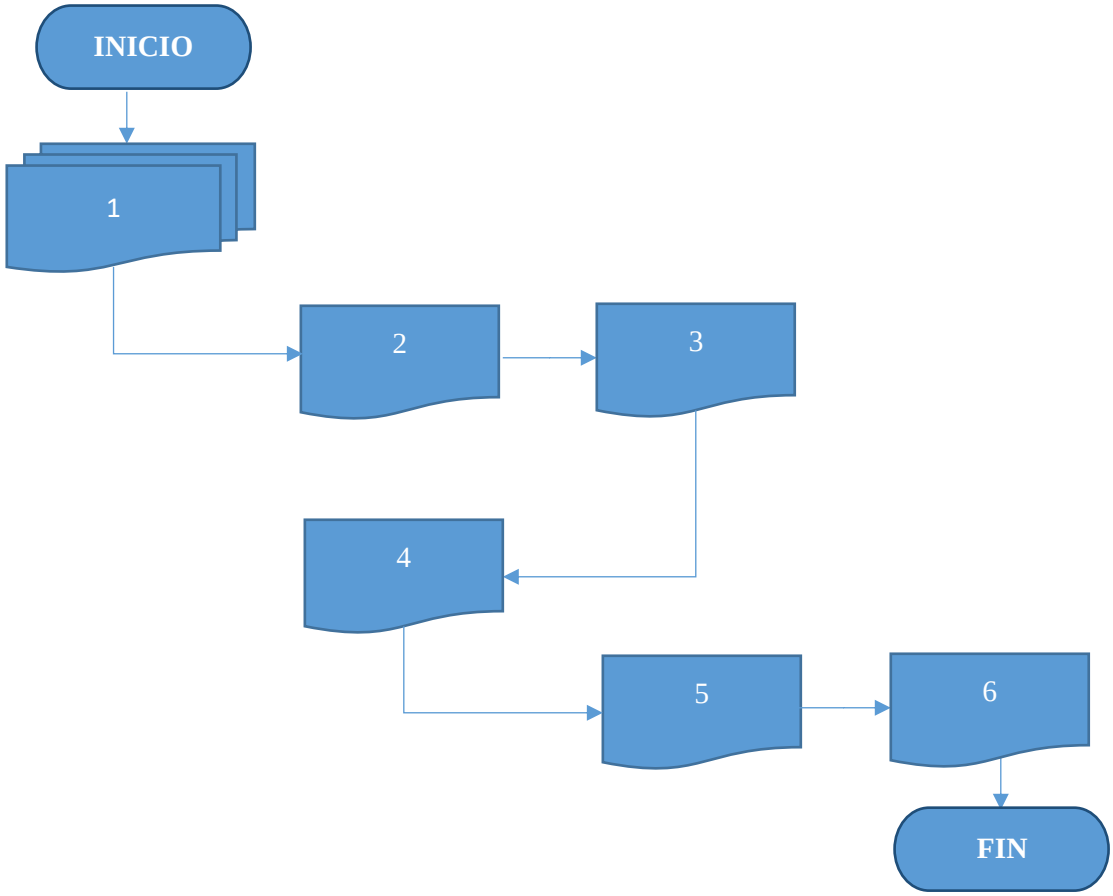
Paso	Responsable	Descripción del procedimiento	Formulario
		a) Intentos de acceso fallidos. b) Bloqueos de cuenta. c) Debilidad de contraseñas. d) Cuentas inactivas y deshabilitadas. e) Últimos accesos a cuentas, entre otros. Registro de uso de los sistemas: a) Accesos no autorizados. b) Uso de Privilegios. c) Alertas de sistema entre otros	
2	Analista/Unidad de Seguridad Informática	-Recibe y revisa el correo electrónico enviado por el sistema automatizado, y notifica al jefe de la Unidad de Seguridad Informática.	Correo electrónico
3	Jefe/ Unidad de Seguridad Informática	-Recibe notificación y asigna el analista que realizará el seguimiento al aviso recibido del sistema.	Correo electrónico
4	Analista/ Unidad de Seguridad Informática	-Recibe las instrucciones e interviene el equipo del funcionario, sin previa autorización del jefe de la unidad administrativa. Nota: Los funcionarios de la unidad de seguridad informática únicamente deben establecer conexiones remotas a través de las VPN seguras y utilizar computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros. -Aísla los equipos o sistemas involucrados (Bloquea la navegación por internet de forma remota). -Verifica el equipo y notifica por escrito al jefe de la unidad las anomalías encontradas y el proceso que se seguirá con la computadora. -Elabora informe sobre el incidente o riesgo encontrado. -Realiza cuestionario al usuario del equipo involucrado. -Realiza análisis al equipo.	AN_USI_03 Informe

Paso	Responsable	Descripción del procedimiento	Formulario
		-Entrega evidencia y recomendaciones al usuario. Nota: El analista realizará revisiones periódicas para la verificación del cumplimiento de los lineamientos. Para efecto, se tendrán en cuenta los registros de eventos y de uso de los sistemas	
5	Jefe/ Unidad de Seguridad Informática	- Recibe el informe con la evidencia de lo encontrado en el análisis del equipo informático. -Envía nota al jefe de la unidad administrativa donde se detectó el riesgo para notificarle de manera formal el hallazgo. -Envía nota a la Dirección de Recursos Humanos, solicitando la aplicación de la respectiva sanción disciplinaria por el mal uso del equipo informático.	Informe Nota codificada
6	Jefe/Unidad Administrativa	-Recibe el informe con la evidencia de lo encontrado en el análisis del equipo informático.	Informe
		FIN DEL PROCEDIMIENTO	

FLUJOGRAMA

PROCEDIMIENTO RESTRICCIÓN DE EQUIPO POR AMENAZA O MAL USO DEL INTERNET

UNIDAD DE SEGURIDAD INFORMÁTICA	ANALISTA/ UNIDAD DE SEGURIDAD INFORMÁTICA	JEFE/UNIDAD DE SEGURIDAD INFORMÁTICA	JEFE/UNIDAD ADMINISTRATIVA



ASAMBLEA NACIONAL
SECRETARÍA GENERAL
DIRECCIÓN DE DESARROLLO INSTITUCIONAL

NOMBRE DEL PROCEDIMIENTO
EVALUACIÓN DE PROYECTOS TECNOLÓGICOS[1]

VERSIÓN DEL PROCEDIMIENTO NO. 1

CÓDIGO
AN_SG_USI_P.A.02

FECHA
15 DE JULIO DE 2023

VALIDADO POR
Ing. Nayubel Ruiz-Jefe
Unidad de Seguridad Informática

DOCUMENTADO POR
Mgtr. Markelda Cañizales-Analista
Dirección de Desarrollo Institucional

DESCRIPCIÓN DEL PROCEDIMIENTO
OBJETIVO:
Garantizar que todos los bienes o servicios tecnológicos adquiridos por la Asamblea Nacional sean eficientes, de calidad y compatible con los sistemas utilizados en la institución.

Unidades administrativas y funcionarios que intervienen en el proceso

Paso	Responsable	Descripción del procedimiento	Formulario
1	Director/Dirección de Tecnología, Informática y Comunicaciones	-Envía nota a la Unidad de Seguridad Informática, para coordinar la evaluación del bien o servicio tecnológico que se va a adquirir.	Nota codificada

[1] Nota: Dependerá de las características de la adquisición que se va a realizar.

La unidad de seguridad informática, realiza una importante aportación al pliego de cargos tales como las garantías, las capacitaciones, los cumplimientos del contrato y el mantenimiento al sistema.

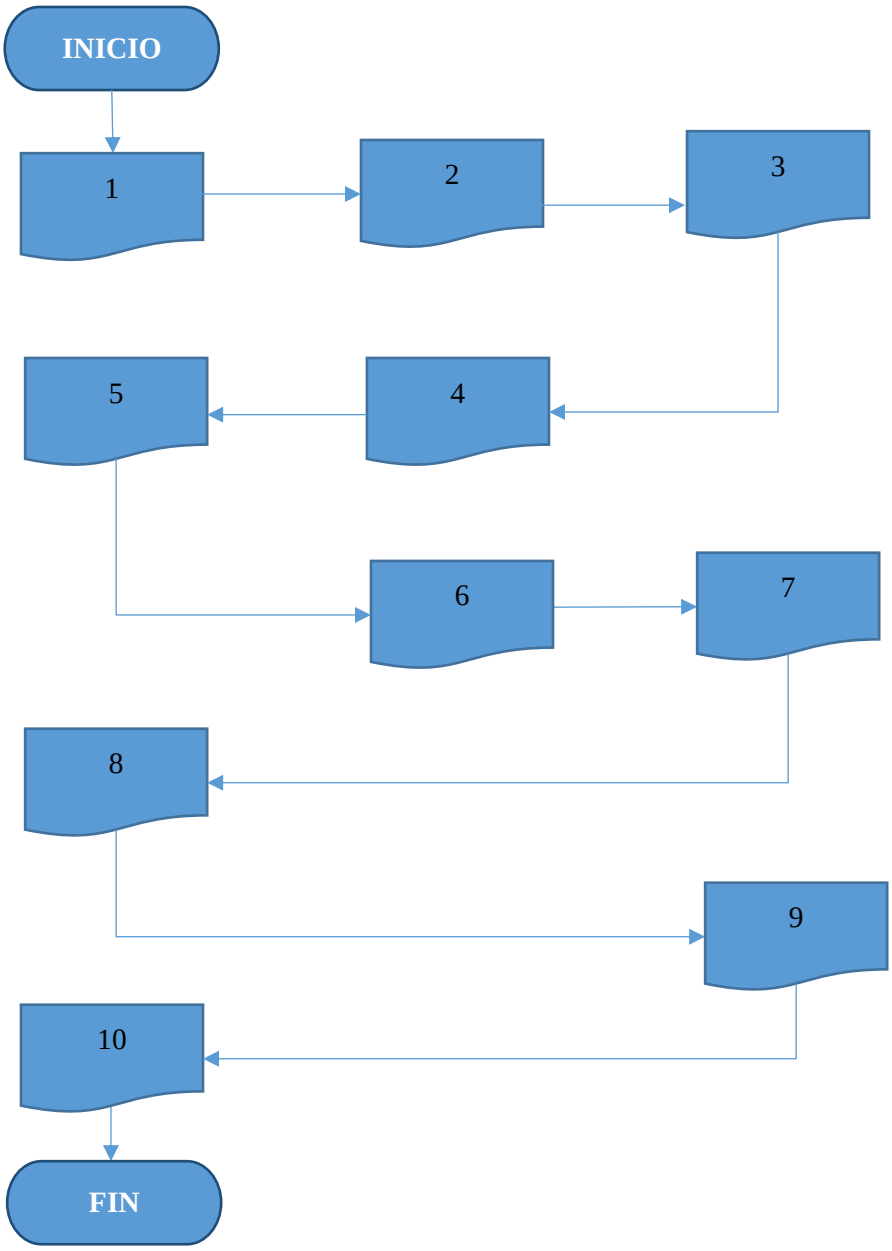
Paso	Responsable	Descripción del procedimiento	Formulario
2	Secretaria/ Unidad de Seguridad Informática	-Recibe y entrega al jefe de la unidad la información recibida.	Nota codificada
3	Jefe/Unidad de Seguridad Informática	-Recibe nota y prepara los términos para ser debatidos -Ordena la lista de recomendaciones. -Solicita a la secretaria prepare nota para enviar la información a la Dirección de Tecnología, Informática y Comunicaciones.	Nota codificada
4	Secretaria/ Unidad de Seguridad Informática	-Recibe las instrucciones y prepara nota remisoria.	Nota codificada
5	Director/Dirección de Tecnología, Informática y Comunicaciones	-Recibe nota con la información detallada proporcionada por la Unidad de Seguridad Informática. -Prepara el pliego de cargos con las (especificaciones del proyecto, garantías, sustentación, objetivos y alcance entre otros detalles), y lo envía a la Unidad de Seguridad Informática.	Pliego de cargos
6	Secretaria/ Unidad de Seguridad Informática	-Recibe y entrega al jefe de la unidad la información recibida.	Nota codificada
7	Jefe/Unidad de Seguridad Informática	-Recibe, verifica, analiza y aporta información sustancial al pliego de cargos. -Remite el análisis de la información a la Dirección de Tecnología, Informática y Comunicaciones.	Pliego de cargos Análisis
8	Director/Dirección de Tecnología,	-Recibe el análisis de la información.	Análisis

Paso	Responsable	Descripción del procedimiento	Formulario
	Informática y Comunicaciones	-Realiza las correcciones necesarias al pliego de cargos. -Organiza reunión de seguimiento para tratar los últimos detalles con relación al pliego. -Presenta al equipo de trabajo el pliego con las acotaciones realizadas.	Pliego de cargos
9	Jefe/Unidad de Seguridad Informática	-Verifica que los puntos sugeridos se encuentren en el pliego de cargos y que el documento tenga la información completa.	Pliego de cargos
10	Director/Dirección de Tecnología, Informática y Comunicaciones	-Presenta el pliego a las autoridades competentes para su Vo.Bo. y posteriormente se realiza la compra.	Pliego de cargos
		FIN DEL PROCEDIMIENTO	

FLUJOGRAMA

PROCEDIMIENTO EVALUACIÓN DE PROYECTOS TECNOLÓGICOS

DIRECTOR/DIRECCIÓN DE TECNOLOGÍA, INFORMÁTICA Y COMUNICACIONES	SECRETARIA/ UNIDAD DE SEGURIDAD INFORMÁTICA	JEFE/UNIDAD DE SEGURIDAD INFORMÁTICA



ASAMBLEA NACIONAL
SECRETARÍA GENERAL
DIRECCIÓN DE DESARROLLO INSTITUCIONAL

NOMBRE DEL PROCEDIMIENTO
AUDITORÍA INFORMÁTICA DE SISTEMAS Y EQUIPOS INFORMÁTICOS ADQUIRIDOS POR LA ASAMBLEA NACIONAL[2]

VERSIÓN DEL PROCEDIMIENTO NO. 1

CÓDIGO
AN_SG_USI_P.A.03

FECHA
15 DE JULIO DE 2023

VALIDADO POR
Ing. Nayubel Ruiz-Jefe
Unidad de Seguridad Informática

DOCUMENTADO POR
Mgtr. Markelda Cañizales-Analista
Dirección de Desarrollo Institucional

DESCRIPCIÓN DEL PROCEDIMIENTO
OBJETIVO:
Asegurar y garantizar la fiabilidad de los sistemas y equipos adquiridos por la Asamblea Nacional, verificando su instalación y utilización por los usuarios internos.

Unidades administrativas y funcionarios que intervienen en el proceso

Paso	Responsable	Descripción del procedimiento	Formulario
1	Jefe/Unidad de Seguridad Informática	-Solicita a la Dirección General de Administración y Finanzas la lista de los equipos, servicios contratados y adquiridos por	Nota codificada

[2] Nota: La auditoría de sistemas se puede realizar por requerimiento o de oficio.

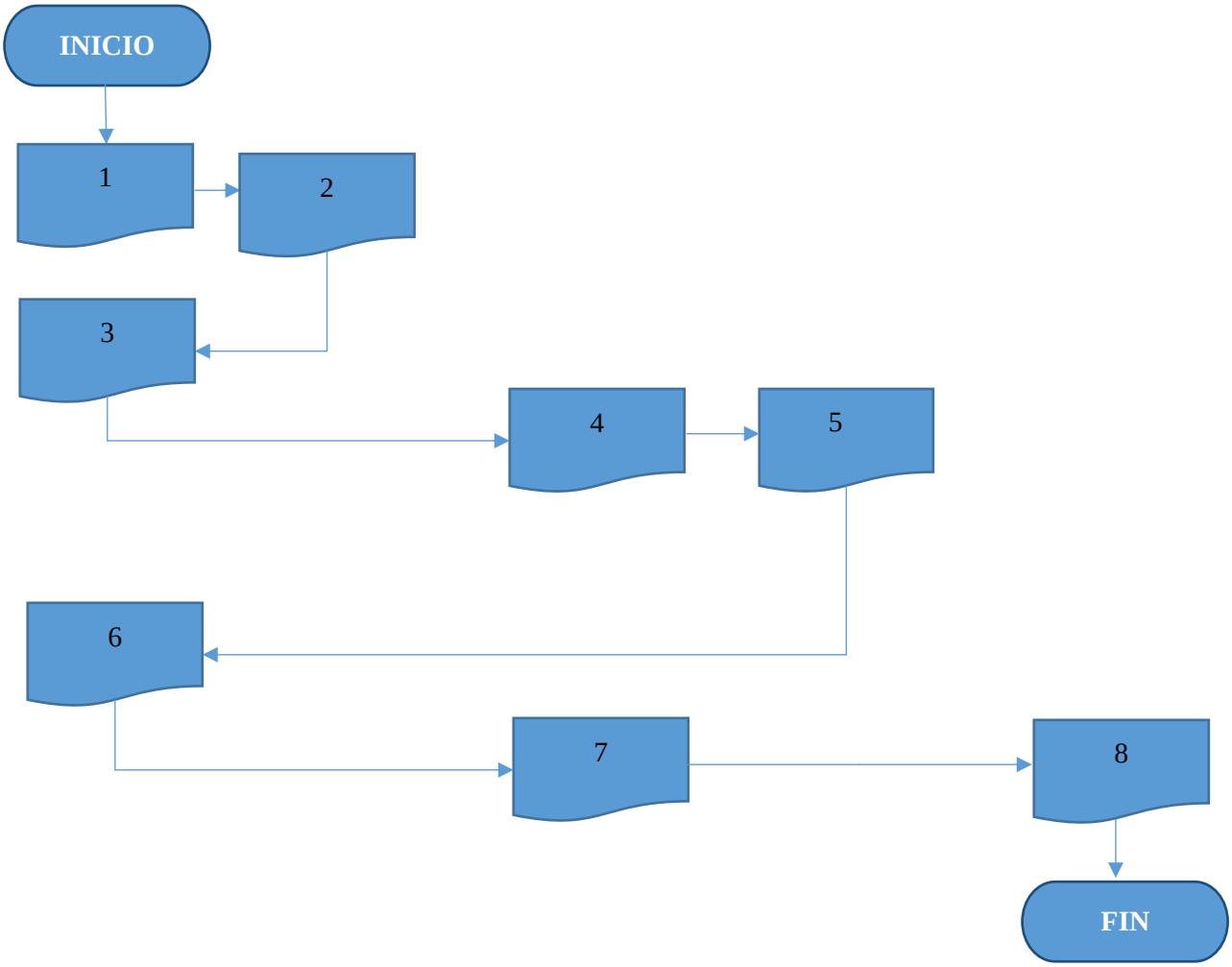
Paso	Responsable	Descripción del procedimiento	Formulario
		la institución en un tiempo específico, por medio de nota.	
2	Director/Dirección General de Administración y Finanzas	-Recibe nota con la solicitud realizada y procede a solicitar dicha información. -Envía la información solicitada.	Nota codificada
3	Jefe/Unidad de Seguridad Informática	-Recibe nota y establece los días para realizar las visitas de inspección según sea el caso. -Asigna a un funcionario para realizar dicha actividad. -Comunica mediante nota a la unidad administrativa, según corresponda el caso, que se realizará una visita programada para verificar la adquisición, uso e implementación del bien o servicio tecnológico adquirido.	Nota codificada
4	Jefe/ Unidad administrativa	-Recibe nota informativa y queda en espera de la inspección establecida.	Nota codificada
5	Analista/Unidad de Seguridad Informática	-Realiza inspección de verificación del bien o servicio tecnológico adquirido. -Entrega informe al jefe inmediato.	Informe de inspección
6	Jefe/Unidad de Seguridad Informática	-Recibe informe, revisa, analiza la información pertinente. -Envía nota al jefe de la unidad administrativa con informe del estado de lo encontrado.	Informe

Paso	Responsable	Descripción del procedimiento	Formulario
7	Jefe/ Unidad administrativa	-Recibe informe del estado de los equipos.	Informe
8	Secretaria/Unidad administrativa	-Recibe y archiva documentación.	Informe
		FIN DEL PROCEDIMIENTO	

FLUJOGRAMA

PROCEDIMIENTO AUDITORÍA INFORMÁTICA DE SISTEMAS Y EQUIPOS INFORMÁTICOS ADQUIRIDOS POR LA ASAMBLEA NACIONAL

JEFE/UNIDAD DE SEGURIDAD INFORMÁTICA	DIRECTOR/ DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS	JEFE/ UNIDAD ADMINISTRATIVA	ANÁLISTA/UNIDAD DE SEGURIDAD INFORMÁTICA	SECRETARIA/ UNIDAD ADMINISTRATIVA



ASAMBLEA NACIONAL
SECRETARÍA GENERAL
DIRECCIÓN DE DESARROLLO INSTITUCIONAL

NOMBRE DEL PROCEDIMIENTO
SOLICITUD DE CAMBIO DE PERFIL DE INTERNET

VERSIÓN DEL PROCEDIMIENTO NO. 1

CÓDIGO
AN_SG_USI_P.A.04

FECHA
15 DE JULIO DE 2023

VALIDADO POR
Ing. Nayubel Ruiz-Jefe
Unidad de Seguridad Informática

DOCUMENTADO POR
Mgtr. Markelda Cañizales-Analista
Dirección de Desarrollo Institucional

DESCRIPCIÓN DEL PROCEDIMIENTO
OBJETIVO:
Analizar el desempeño y funcionamiento de la Red (Internet) por parte del usuario, a fin de lograr la utilización eficiente y segura de la información.

Unidades administrativas y funcionarios que intervienen en el proceso

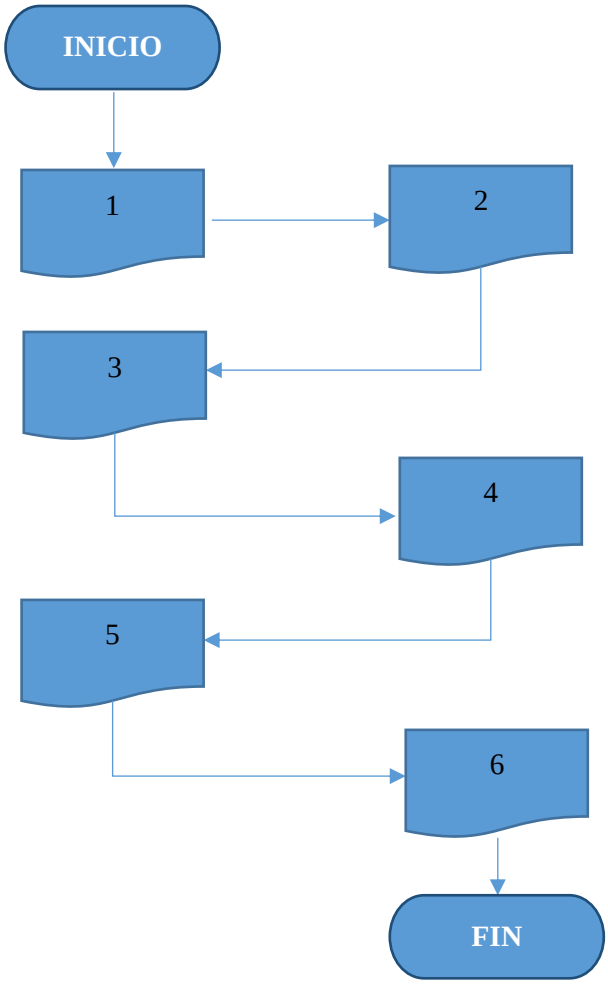
Paso	Responsable	Descripción del procedimiento	Formulario
1	Unidad Administrativa/ Solicitante	-Remite mediante nota o correo electrónico a la Unidad de Seguridad Informática, solicitud de cambio de perfil de internet.	Nota codificada correo electrónico
2	Analista/ Unidad de Seguridad Informática	-Recibe nota o correo electrónico de la unidad solicitante.	Nota codificada correo electrónico AN_SG_USI_14

Paso	Responsable	Descripción del procedimiento	Formulario
		-Verifica la solicitud y realiza análisis correspondiente. -Remite formulario de control de uso de internet.	
3	Unidad Administrativa/ Solicitante	-Recibe y completa el cuestionario correspondiente. -Remite cuestionario con la información solicitada por la Unidad de Seguridad Informática.	AN_SG_USI_14
4	Analista/Unidad de Seguridad Informática	-Recibe cuestionario debidamente completado. -Evalúa y procede a ejecutar la solicitud de acceso o negación de la solicitud. -Revisa el Firewall para el control de aplicaciones y filtrado de web (habilitar o deshabilitar). -Verifica tipo de usuario y confirma las aplicaciones permitidas al usuario. -Comprueba el sistema operativo (si necesita actualización o no). -Establece las aplicaciones de control (antivirus o anti SPAM).	AN_SG_USI_14
5	Unidad Administrativa/ Solicitante	-Usuario firma las políticas sobre el uso del internet y nota de aceptación.	AN_SG_USI_14
6	Analista/Unidad de Seguridad Informática	Remite informe a Secretaría General.	Nota codificada
		FIN DEL PROCEDIMIENTO	

FLUJOGRAMA

PROCEDIMIENTO SOLICITUD DE CAMBIO DE PERFIL DE INTERNET

UNIDAD ADMINISTRATIVA/ SOLICITANTE	ANALISTA/UNIDAD DE SEGURIDAD INFORMÁTICA



VIII

· FORMULARIOS

Código AN_USI_01
Versión 01
Fecha versión 12-jun-2023

UNIDAD DE SEGURIDAD INFORMÁTICA

CONTROL DE MANEJO DE INFORME TÉCNICO

Departamento:_____ **Fecha:**_____

Funcionario Responsable:_____ **Hora:**_____

Trabajo solicitado por:_____

Motivo de la Solicitud:	
Auditoría	
Soporte	
Monitoreo	
Incidente	

Procedimiento a Realizar:

Sistema Afectado:

Estatus de trabajo realizado:

Verificado Por: _____

Duración del Trabajo: _____

Personal Externo (de ser necesario)					
Nombre	**Cédula**	**Empresa**	**Fecha**	**Hora**	**Firma**

UNIDAD DE SEGURIDAD INFORMÁTICA
CONTROL DEL ACCESO A INFORMACIÓN TÉCNICA

Código AN_USI_02
Versión 01
Fecha versión 12-jun-2023

Funcionario responsable de la entrega de información:_____

Datos del Solicitante:
Nombre y Cédula:_____
Empresa:_____
Firma:_____

Activo a Revisar			
Servidor		Cableado AP Switches	
Base de Datos		Red de Datos	
Software de aplicación, proc, fuentes		Usuarios	
Sistema Operativo		Doc. de Programas, Soft Harw	
Backup		Doc. de Sistemas Proc Admón., Manuales	
Datos de Configuración		Insumos (Tinta, Tóner)	
Datos en medios Externos (USB, Disco)		Internet Inalámbrico	
Hardware		Correo Electrónico	
		Istmo	

Motivo de la Solicitud:	
Acceso para consulta	
Cambio	
Entrega	
Backup	
Verificación	

PROCEDIMIENTO A REALIZAR	

VERIFICADO POR:	

Código AN_USI_03
Versión 01
Fecha de versión 12-Jun-2023

Unidad de Seguridad Informática
Informe de bloqueo de IP

Fecha:	
IP:	
Motivo:	
Pagina web:	
Tiempo de Bloqueo:	
Inspector:	

Imagen de Muestra

Código AN_USI_04
Versión 01
Fecha de versión 12-Jun-2023

Unidad de Seguridad Informática

Bitacora de servicio

Fecha de revisión:	
Nombre de usuario:	
Nombre de equipo:	
Departamento:	
Nombre de funcionario:	

Bitacora N°

Descripción del equipo		
IP		
Sistema operativo		
Antivirus		
Office		
Número de equipo		

Problema encontrado:

- ☐ Antivirus desactualizado
- ☐ Windows desactualizado
- ☐ No tiene antivirus
- ☐ IP Bloqueado
- ☐ Problemas de navegación
- ☐ Cambio de IP
- ☐ Malware
- ☐ otros

Solución:	**Comentarios:**

Firma del inspector:

Código AN_USI_05
Versión 01
Fecha de versión 12-Jun-2023

Unidad de Seguridad Informática

Informe de Correos Maliciosos

Fecha:	
Dirección de Correo:	
Accion realizada:	
Inspector:	

Foto de muestra

Código AN_USI_06
Versión 01
Fecha de versión 12-jun-2023

UNIDAD DE SEGURIDAD INFORMÁTICA
CONTROL DE AUDITORIA

Nº De Placa:_____

Inspector:_____ Fecha:_____ Hora:_____

CONTROL ORGANIZACIONAL 10%

UNIDAD ADMINISTRATIVA:_____ JEFE ENCARGADO:_____

UBICACIÓN

EDIF. VIEJO
PISO _____

EDIF. 356
MÓDULO _____

EDIF. NUEVO
PISO _____

REDES Y COMUNICACIONES 20%

NOMBRE DE EQUIPO
_____

NOMBRE DE USUARIO
_____

TIPO DE CUENTA
ADMINISTRADOR ☐
LIMITADO ☐

CONTRASEÑA
GENERICA ☐
PERSONAL ☐

ÚLTIMO CAMBIO DE CONTRASEÑA
1-6 MESES ☐
6-12 MESES ☐
12 MESES O MAS ☐

TIENE INTERNET
SÍ ☐
NO ☐

TIPO DE CONEXIÓN
UTP ☐
INALAMBRICA ☐

IP/RED
_____

DIRECCION MAC
_____

DOMINIO
AN LOCAL ☐
ASAMBLEA.GOB.PA ☐

IP BLOQUEADA EN EL FIREWALL
SÍ ☐
NO ☐

IP REGISTRADA EN EL FIREWALL
SÍ ☐
NO ☐

CARPETA COMPATIDA
SÍ ☐
NO ☐

OBSERVACIÓN:_____

NOMBRE:_____

CORREO ELECTRONICO
SÍ ☐
NO ☐

BANDEJA DE CORREO
_____

VELOCIDAD DE CONEXIÓN
_____

EQUIPOS DAÑADOS EN LA UNIDAD
_____

APLICACIONES 25%

OFFICE/VERSION
SÍ ☐
NO ☐
VERSION:
_____

BASE DE DATOS
SÍ ☐
NO ☐
VERSIÓN:
_____

SAP
SÍ ☐
NO ☐
VERSION:
_____

ANTIVIRUS
SÍ ☐
NO ☐
VERSION:
_____

SISTEMA OPERATIVO
WINDOWS ☐
LINUX ☐
OTRO:
_____

OBSERVACIONES:_____

ULTIMA FECHA DE MANTENIMIENTO
1-6 MESES ☐
6-12 MESES ☐
12 MESES O MÁS ☐

SEGURIDAD FÍSICA/LÓGICA 45%

ID DE RIESGO	☐
SIN ANTIVIRUS	☐
ANTIVIRUS DESACTUALIZADO	☐
SIN ACTUALIZACIONES DE WINDOWS	☐
SIN BACKUP LOCAL/SERVER	☐
CONTRASEÑA GENÉRICA	☐
USUARIO GENÉRICO	☐
USUARIO ADMINISTRADOR	☐
CARPETAS COMPARTIDAS	☐
APLICACIONES DESACTUALIZADAS	☐

UNIDAD DE SEGURIDAD INFORMÁTICA

Código AN_USI_07
Versión 01
Fecha de versión 12-jun-2023

ENCUESTA PARA EVALUAR EL USO DE LOS SISTEMAS DE INFORMACIÓN

Esta encuesta tiene como objetivo conocer sobre los sistemas de información que posee la unidad administrativa a su cargo, su funcionamiento y el cumplimiento de las metas definidas durante su implementación, así como también conocer sobre las nuevas exigencias tecnológicas que ha de requerir.

UNIDAD ADMINISTRATIVA: _____

JEFE O ENCARGADO: _____

FECHA: _____ HORA: _____

REALIZADO POR: _____

Responda las preguntas de manera clara y sencilla. Puede solicitar ayuda de algún colaborador.

1. ¿Qué sistemas de información se utilizan actualmente en unidad administrativa que usted dirige, qué áreas los utilizan? Enumere.
2. ¿En qué porcentaje de aplicación se encuentran los sistemas de información actuales?
3. ¿Cuáles serían las metas y objetivos principales que a usted le gustaría cubrir con un sistema de información usando tecnología? Enumere.
4. ¿Cómo evalúa el desempeño de sus sistemas de información en la actualidad? Explique brevemente.
5. ¿Quién es el encargado de encontrar y evaluar las tecnologías de información que más se ajusten a sus actividades diarias?
5. ¿Cuáles son los procesos que considera medulares en cuanto al manejo de la información de su área administrativa?
6. ¿Cuáles son los procesos que considera medulares en cuanto a la toma de decisiones?
7. ¿Qué características debería tener el sistema de información que le apoyará en la toma de decisiones?
8. ¿Qué información le proporciona su sistema de información actual?
9. ¿Qué reportes genera su sistema actual?
10. ¿Qué reportes le gustaría tener que ahora no tiene?
11. ¿Su sistema permite que otras personas puedan ver la misma información simultáneamente desde otras computadoras?

Código AN_USI_08
Versión 01
Fecha de versión 12-jun-2023

UNIDAD DE SEGURIDAD INFORMÁTICA
MANTENIMIENTO

Orden de Servicio Nº ____

Tipo de Servicio ☐ **Garantía** ☐ **Contrato** ☐ **Costo M/O**

Condiciones de pago: ☐ **Contado** ☐ **Crédito**

Proveedor:_____ **Contacto:**_____

Dirección:_____ **Teléfono:**_____

Tipo de Equipo:_____ **Marca:**_____ **Serie:**_____

AFECTACIONES REPORTADAS POR EL CLIENTE: **Hora de Inicio:**_____

_____ **Hora de Culminación:**_____

DESCRIPCIÓN DEL TRABAJO REALIZADO

_____
_____
_____
_____
_____

OBSERVACIONES/ RECOMENDACIONES

_____
_____
_____
_____
_____

SERVICIO RECIBIDO POR:

_____
REALIZADO POR

_____ _____
NOMBRE FIRMA

Código AN_USI_11
Versión 0
Fecha de versión 12-jun-2023

Unidad de Seguridad Informática

ENCUESTA DE SATISFACCIÓN DE USUARIO FINAL

Encierre en un círculo la respuesta que de manera objetiva más se identifique con su opinión.

1. **¿Está satisfecho con la gestión que realiza la Asamblea Nacional en temas de tecnología?**

   a. Nunca satisfecho b. Poco satisfecho c. Satisfecho d. Muy satisfecho

2. **¿El servicio de técnico de la Asamblea Nacional cuando lo ha necesitado cumple con sus expectativas?**

   a. Nuncab. b veces c. Normalmente d. Casi siempre e. Siempre

3. **¿El servicio de soporte brindado por la Asamblea Nacional ha resuelto su necesidad específica?**

   a. Nunca b. A veces c. Normalmente d. Casi siempre e. Siempre

4. **¿Al solicitar el servicio técnico de la Asamblea Nacional en qué tiempo se responde su solicitud?**

   a. Minutos b. Horas c. Semanas d. Meses e. No llega

5. **¿El personal de tecnología que le atiende responde sus consultas o preguntas técnicas?**

   a. Nunca b. A veces c. Normalmente d. Casi siempre e. Siempre

6. **¿La atención brindada y la capacidad, mostrada del personal técnico le transmite seguridad?**

   a. Nunca b. A Veces c. Normalmente d. Casi siempre e. Siempre

Código AN_USI_09
Versión 01
Fecha de versión 12-jun-2023

UNIDAD DE SEGURIDAD INFORMÁTICA

PROGRAMA DE MANTENIMIENTO

Nombre	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Observaciones
Antivirus Antimalware													
Protección de virus y afectaciones de archivos, equipos de la institución													
Anti-SPAM													
Protección de correos electrónicos contra virus, phising, suplantación de identidad, de la institución.													
Forti-Analyzer													
Sistema de Reportes, para los equipos de la marca fortinet.													
Fortigate-Firewall													
Protección perimetral de toda la red, ante ataques en intrusiones a información de la institución.													

Unidad de Seguridad Informática

Código AN_USI_13
Versión 0
Fecha de versión 12-Jun-2023

SOLICITUD DE ACCESO AL SERVICIO VPN

Tipo de solicitud

Primera vez: ☐ **Renovación:** ☐

Fecha Solicitud:	Fecha Inicio del Servicio:	Fecha Fin del Servicio:

Destinatario final de acceso a la VPN:

Empresa:	**Nombre:**	**Apellido:**
Dpto:		**Céd:**
Teléfono:	**Email:**	
Motivo:		

APROBADO por (responsable Unidad de Seguridad Informática):

Nombre:	**Apellido:**
Cargo:	
Teléfono:	**Email:**
Firma autorizada:	**Fecha:** **Documento de Control No.:**

OBSERVACIONES:

- Los datos de conexión (usuario y contraseña), se comunicarán directamente al destinatario final de acceso a la VPN.
- Los accesos a los servidores y servicios, no se solicitan en este formulario. Serán proporcionados por la DITIC.
- Para tramitar esta solicitud de acceso al servicio de VPN institucional, deberá referirse a la USI.
- La conexión solo permitirá tener acceso a aquellos servidores de la red informática que se autoricen por parte de la DITIC.
- El usuario VPN no podrá acceder a los recursos de su red local (carpetas o impresoras compartidas en otros equipos de la red local) y no podrá navegar por internet ni recibir/enviar correo electrónico a menos que utilice el servicio de correo institucional con la debida autorización y control de la USI y la DITIC.

Código AN_USI_14
Versión 01
Fecha de versión 12-jun-2023

CONTROL DEL USO DEL INTERNET

1. ¿CON QUÉ FRECUENCIA USA INTERNET?
   a. 1 día a la semana.
   b. 3 días a la semana.
   c. Todos los días.

2. ENUMERE 5 FUNCIONES DENTRO DE LA UNIDAD ADMINISTRATIVA
   a._____
   b.-_____
   c._____
   d._____
   e. _____

3. ¿QUÉ TIPO DE PÁGINAS VISITA CON MÁS FRECUENCIA?

NUMERAR DE 1 A 7 (1=LA MÁS VISITADA; LA MENOS VISITADA)

   a. Noticias, prensa, correo electrónico personal _____
   b. Redes Sociales (Facebook, LinkedIn, Instagram, Tik Tock) _____
   c. Entretenimiento (YouTube, juegos) _____
   d. Descarga de Archivos _____
   e. Recursos educativos Wikipedia, blogs, foros educativos _____
   f. Servicios (Banca en línea, escuelas, pagos)
   g. Recursos Varios (páginas web gubernamentales, extranjeras, Google _____

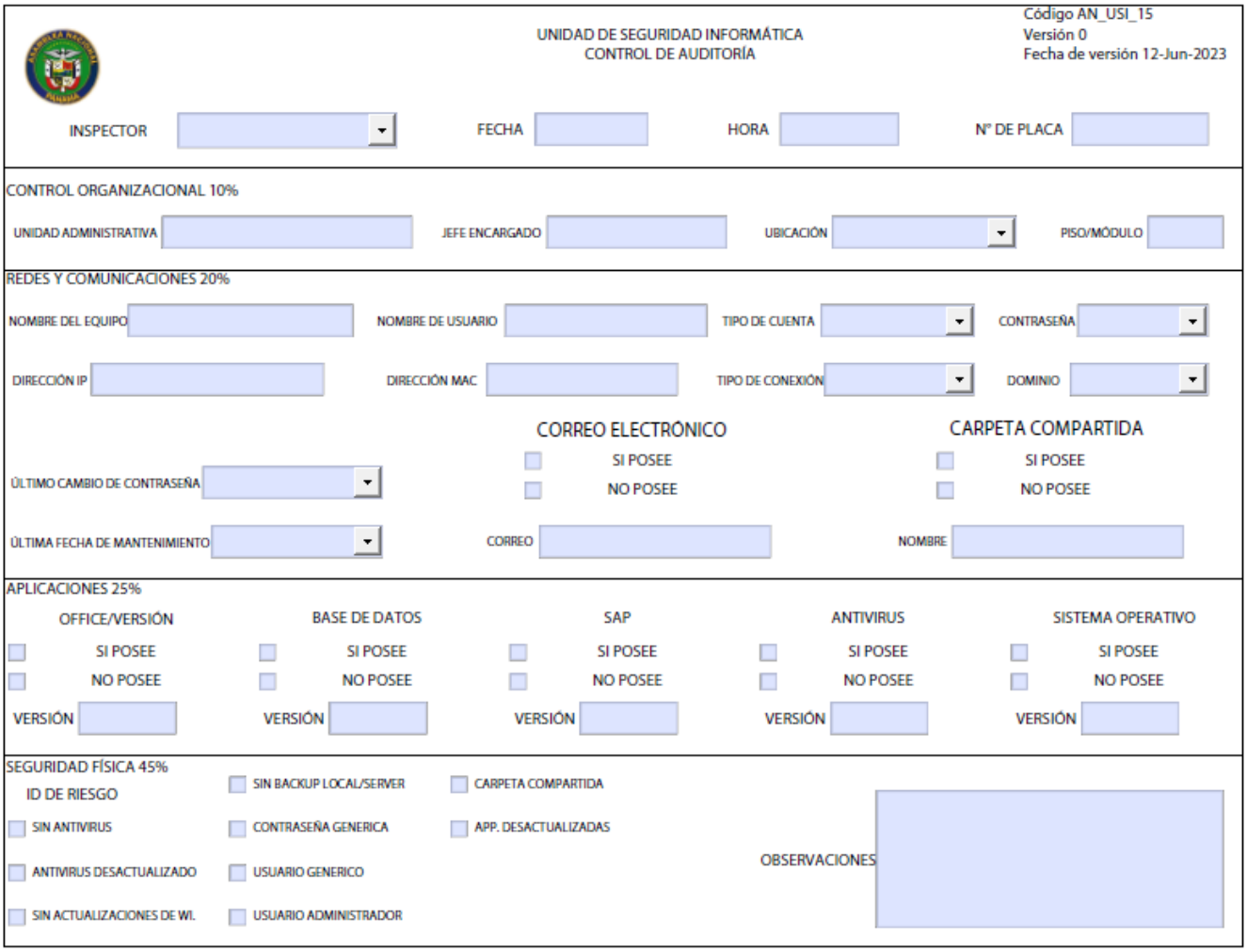
4. DE LAS PREGUNTAS ANTERIORES MENCIONE, ¿CUÁLES CONSIDERA USTED SON LAS PÁGINAS VISITADAS MÁS RELEVANTES CON SUS FUNCIONES?
   a. _____
   b. _____
   c. _____
   d. _____

5. DE LA PREGUNTA 4, EXPLIQUE BREVEMENTE, ¿QUÉ TIPO DE APOYO LE DA A SUS FUNCIONES CADA UNA DE LAS RESPUESTAS MENCIONADAS?
   a. _____
   b. _____
   c. _____
   d. _____

6. DE LA PREGUNTA 3, ¿MENCIONE CUÁLES PÁGINAS VISITADAS CONSIDERA USTED IRREVENTANTE EN SUS FUNCIONES?
   a. _____
   b. _____
   c. _____
   d. _____

7. ¿CONSIDERA USTED QUE EL INTERNET LE SIRVE DE APOYO EN SUS FUNCIONES DIARIAS?
   a. Nunca
   b. A veces
   c. Con frecuencia
   d. Siempre

8. ¿ADEMÁS DEL USO QUE LE DA AL INTERNET PARA SUS FUNCIONES DIARIAS, PARA QUÉ OTRA ACTIVIDAD LA UTILIZA?
   a. Buscar información para trabajos (escolares, universitarios)
   b. Aclarar dudas, investigaciones, cursos (en foros, Wikipedia)
   c. Diccionarios, traductores.
   d. Otros_____



UNIDAD DE SEGURIDAD INFORMÁTICA
CONTROL DE AUDITORÍA

Código AN_USI_15
Versión 0
Fecha de versión 12-Jun-2023

INSPECTOR | FECHA | HORA | N° DE PLACA

CONTROL ORGANIZACIONAL 10%

UNIDAD ADMINISTRATIVA | JEFE ENCARGADO | UBICACIÓN | PISO/MÓDULO

REDES Y COMUNICACIONES 20%

NOMBRE DEL EQUIPO | NOMBRE DE USUARIO | TIPO DE CUENTA | CONTRASEÑA

DIRECCIÓN IP | DIRECCIÓN MAC | TIPO DE CONEXIÓN | DOMINIO

ÚLTIMO CAMBIO DE CONTRASEÑA

CORREO ELECTRÓNICO
SI POSEE
NO POSEE

CARPETA COMPARTIDA
SI POSEE
NO POSEE

ÚLTIMA FECHA DE MANTENIMIENTO | CORREO | NOMBRE

APLICACIONES 25%

OFFICE/VERSIÓN	BASE DE DATOS	SAP	ANTIVIRUS	SISTEMA OPERATIVO
SI POSEE	SI POSEE	SI POSEE	SI POSEE	SI POSEE
NO POSEE	NO POSEE	NO POSEE	NO POSEE	NO POSEE
VERSIÓN	VERSIÓN	VERSIÓN	VERSIÓN	VERSIÓN

SEGURIDAD FÍSICA 45%

ID DE RIESGO

- SIN ANTIVIRUS
- ANTIVIRUS DESACTUALIZADO
- SIN ACTUALIZACIONES DE WI.
- SIN BACKUP LOCAL/SERVER
- CONTRASEÑA GENERICA
- USUARIO GENERICO
- USUARIO ADMINISTRADOR
- CARPETA COMPARTIDA
- APP. DESACTUALIZADAS

OBSERVACIONES

FIRMAS

El presente Manual de Procedimientos Administrativos de la Unidad de Seguridad Informática ha sido avalado por los siguientes responsables:

Documentado por: **Mgtr. Markelda Cañizales** Analista de la Dirección de Desarrollo Institucional	•
Revisado por: **Ing. Nayubel Ruiz** Jefe de la Unidad de Seguridad Informática	•
Revisado por: **Lcda. Luz Marina Navarro** Directora de Desarrollo Institucional	•
Aprobado por: **Lcdo. Quibián T. Panay G.** Secretario General	•

REPÚBLICA DE PANAMÁ SECRETARÍA GENERAL ASAMBLEA NACIONAL

IX. HISTORIAL DE CAMBIOS

	SECRETARÍA GENERAL **DIRECCIÓN DE DESARROLLO INSTITUCIONAL**	Código AN_DDI_07 Versión 01 Fecha de versión 10-jul-2023
	HISTORIAL DE CAMBIOS	

Naturaleza del cambio	Fecha	Revisión
Manual de Procedimiento Administrativo, última versión.	2017	0
• Cambio al formato siguiendo los parámetros de la norma de ISO 9001:2015. • Cambio en el flujo de los procedimientos	2023	1