GOBIERNO DE EL SALVADOR

COMISIÓN NACIONAL DE LA MICRO Y PEQUEÑA EMPRESA

MANUAL DE METODOLOGÍA, LINEAMIENTOS Y POLÍTICAS INFORMÁTICAS

2020

GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

www.conamype.gob.sv

Contenido

BASE LEGAL

Los fundamentos legales que dan origen al presente Manual están contenidos en:

a) Ley de Fomento, Protección y Desarrollo para la Micro y Pequeña Empresa; Decreto Legislativo No.667, de fecha 25 de abril de 2014, publicado en el Diario Oficial No. 90, Tomo No. 403 del 20 de mayo del mismo año.

b) Reformas emitidas en el Decreto Legislativo No. 838 de fecha quince de noviembre del año dos mil diecisiete, artículo diez-g, letra k), establece que es atribución de la Junta Directiva: "Autorizar los reglamentos operativos, manuales de organización, funciones, descriptores de puestos, procesos y otros necesarios para el buen funcionamiento institucional".

c) Reglamento de Normas Técnicas de Control Interno de la Corte de Cuentas de La República, según Decreto No. 1 de fecha 16 de enero de 2018.

d) Decreto No. 24 de fecha 8 julio de 2014 emitido por la Corte de Cuentas de la República; Reglamento Para El Uso Y Control De Las Tecnologías De Información Y Comunicación En Las Entidades Del Sector Público

ALCANCE

El cumplimiento a las disposiciones contenidas en el presente documento es responsabilidad de todo el personal que labora en CONAMYPE, inclusive las personas externas relacionadas con el desarrollo de las actividades institucionales para hacer uso de los recursos tecnológicos de CONAMYPE deberán prestar observancia a la normativa contenida en este documento, para lo cual, la Gerencia de Tecnologías de la Información será quien coordine y lidere la aplicabilidad, como administrador de las bases de datos, de la estructura instalada y regulador de los contenidos en uso a través de aplicativos.

METODOLOGÍA PARA EL DESARROLLO DE SISTEMAS

METODOLOGÍA PARA EL DESARROLLO DE SISTEMAS

Análisis de Requerimientos.

El desarrollo de un sistema informático parte del análisis inicial el cual debe tratar de descubrir los requerimientos del producto al cual se desea solucionar mediante una aplicación informática. Unos de los principales objetivos es hacer que este análisis sea lo suficientemente intuitivo para que los clientes y expertos en el dominio del problema que solicitan el producto puedan comprenderlo, y lo suficientemente formal y riguroso para que se establezca una formulación no ambigua que pueda ser utilizada por los técnicos que la desarrollan.

Contexto y Objetivos

Se debe describir la situación actual del problema, el entorno, cual es el objetivo general y los objetivos específicos.

Especificación del Problema

Se deben de describir cada uno de los procesos de los problemas que se quieren solucionar. Se define de forma completa, precisa y verificable, los requisitos, el diseño y el comportamiento u otras características del problema a solucionar. Para realizar bien el desarrollo de software es esencial tener una especificación completa de los requerimientos.

Las especificaciones del problema se obtienen a partir de entrevistas y reuniones con la jefatura inmediata la cual tiene el problema que es necesario sistematizar, así con los técnicos expertos en el tema que son delegados por el jefe.

Los requerimientos se representan de forma que conduzcan finalmente a una correcta implementación del software. [Sommerville, 2005] plantea que una buena especificación debe procurar:

- Separar funcionalidad de implementación. Una especificación es una descripción de lo que se desea, en vez de como se realiza. Esto en la práctica puede llegar a no suceder del todo, sin embargo, es un buen lineamiento a seguir.

- Una especificación debe abarcar el entorno en el que el sistema opera. Similarmente, el entorno en el que opera el sistema y con el que interactúa debe ser especificado.

- Debe ser modificable. Ninguna especificación puede ser siempre totalmente completa. El entorno en el que existe es demasiado complejo para ello. Una especificación es un modelo, una abstracción, de alguna situación real (o imaginada). Por tanto, será incompleta. Además, al ser formulada existirán muchos niveles de detalle.

Resultado Inicial

El primer resultado esperado es un documento describiendo contexto, objetivos y problema. En el detalle cada problema se debe especificar el tema de este y la correspondiente descripción.

Dominio del problema.

El modelo de dominio puede ser tomado como el punto de partida para el diseño del sistema. Esto es así porque, cuando se realiza la programación, se supone que el funcionamiento interno del software va a imitar en alguna medida a la realidad, por lo que el mapa de conceptos del modelo de domino constituye una primera versión del sistema. El objetivo es capturar lo necesario para comprender donde va a funcionar el sistema que estamos diseñando y esto demanda una cantidad distinta de detalles cada vez.

Conceptos de Entidades de datos: clases y atributos.

Identificación de todas las entidades que se incluyen en el dominio del problema, con una breve descripción e incluir si será una clase o atributo. Los conceptos no son propios del sistema a elaborar sino del problema a resolver.

Diagrama del Dominio del Problema.

Diagrama que relaciona todas las diferentes entidades comprendidas en el dominio del problema indicando cual es la relación entre ellos y su cardinalidad.

Resultado del Dominio del Problema

El segundo resultado, no es un nuevo documento, consiste en enriquecer el documento inicial para que esta se convierta en el documento de análisis del problema. En esta etapa se modificará el problema, si es necesario se modifica la descripción, y por cada problema se adicionan los conceptos de entidades y el diagrama del dominio de cada problema.

Requerimientos Funcionales

La especificación debe contener los requerimientos del sistema, la IIEEE 29148-2011[1], divide los requerimientos en funcionales y no funcionales. Los requerimientos funcionales describen una interacción entre el sistema y su ambiente, describen cómo debe comportarse el sistema ante determinado estímulo. Son declaraciones de los servicios que debe proporcionar el sistema, de la manera en que éste debe reaccionar a entradas particulares y de cómo se debe comportar en situaciones particulares. En algunos casos, también pueden declarar explícitamente lo que el sistema no debe hacer. Los requerimientos funcionales de un sistema describen lo que el sistema debe hacer.

[1] IEEE 29148-2011 - ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes --Requirements engineering. https://standards.ieee.org/standard/29148-2011.html

Listado de Requerimientos funcionales.

Para la documentación de los requerimientos podemos empezar agrupándolos por módulos funcionales, asignar código a cada módulo y a cada requerimiento para facilitar su búsqueda, ya sea al momento de realizar la implementación o al momento de realizar cambios.

COD01	NOMBRE DEL MODULO 1
COD01-01	PROCESO 1 MODULO 1
COD01-02	PROCESO 2 MODULO 1
COD02	**NOMBRE DEL MODULO 2**
COD01-01	PROCESO 1 MODULO 2
COD01-02	PROCESO 2 MODULO 2
COD01-XX	PROCESO …

Definición de Actores/Usuarios

Los actores representan un tipo de objeto externo al sistema pero que interacciona con él. Un objeto puede implementar varios actores, y cada actor puede tener múltiples implementaciones. Los actores pueden ser:

- Actores principales: Usuarios que utilizan las funciones principales del sistema.
- Actores secundarios: Personas que efectúan tareas administrativas o de mantenimiento del sistema.
- Elementos externos: Equipos y dispositivos que forman el ámbito de la aplicación pero que no se desarrollan con ella.
- Otros sistemas: Sistemas externos al que se desarrolla que interactúan con él.

Para describir los actores utilizamos la siguiente tabla:

ACTOR	CLASIFICACIÓN	DESCRIPCIÓN
Nombre del Actor 1	Principal / Secundario / Externo / Sistema	Descripción del rol del actor.
Nombre del Actor X	Principal / Secundario / Externo / Sistema	Descripción del rol del actor.

Casos de Uso.

Para cada uno de los requerimientos deben de describirse su comportamiento, entradas particulares y situaciones particulares. Para describir los requerimientos se utilizarán los casos de uso, indicando el código del requerimiento que se describe.

Los casos de uso describen cosas que los actores quieren que el sistema haga. Un caso de uso debe ser una tarea completa desde el punto de vista del actor, y debe corresponder a una tarea que se realiza en un tiempo relativamente breve, especialmente si debe ser realizado por múltiples actores. Cuando estas condiciones no se cumplen, es mejor definir varios casos de uso independientes.

Un caso de uso describe no solo una funcionalidad o una motivación, sino también una interacción entre un actor y el sistema bajo la forma de un flujo de eventos. La descripción que proporciona el caso de uso se refiere a lo que se espera que la interacción realice y no a como lo realiza. Los componentes, la descripción de estos y el formato como se documentan se presenta en la siguiente tabla:

01 (No. del CU)	COD01-01	NOMBRE	CREACION DE ROLES
DESCRIPCIÓN		Descripción del Proceso	
ACTORES		Listado de Actores que participan en el proceso	
PRE-CONDICION		Condiciones que se deben de cumplir para iniciar el proceso	
PROCESAMIENTO		**Flujo Ideal**	
		1- Listado de tareas a realizar en el proceso si todo sale bien 2- …	
		Flujo alterno	
		2. A.1. Listado de tareas que se realizan cuando falla una tarea del flujo ideal en el punto 2. 2. A.2 … 2. B.1. Listado de tareas que se realizan cuando falla una tarea del flujo ideal en el punto 2. 2. B.2 … 4. A.1 …	
REGLAS DEL NEGOCIO		Regla del negocio a cumplir	
POST CONDICION		Condiciones que genera el proceso. Pueden ser las precondiciones de otro proceso.	
CRITERIO DE ACEPTACION		Criterios que debe de cumplir el proceso para ser válido.	

Requerimientos no Funcionales

Sommerville, en la edición del 2005[2], desglosa los tipos de requerimientos no funcionales. Los tres grupos generales son: requerimientos del producto, organizacionales y externos, de cada grupo se derivan los particulares.

- Requerimientos del Producto: Especifican el comportamiento del producto. Ejemplos: rapidez de la ejecución, capacidad de memoria, fiabilidad, etc.
- Requerimientos Organizacionales: Derivan de políticas y procedimientos existentes en la organización del cliente y del desarrollador. Ejemplos: Estándares de procesos, métodos de diseño, lenguajes de programación, métodos de entrega, etc.
- Requerimientos Externos: Se derivan de factores externos al sistema y de sus procesos de desarrollo. Ejemplos: Requisitos de interoperabilidad, legislativos, éticos, etc.

Para documentar los requisitos no funcionales utilizamos la siguiente tabla, con los componentes y la descripción del contenido:

01 (No. RNF)	COD.RNF-1	NOMBRE	Nombre del requerimiento no funcional
DESCRIPCIÓN		Descripción del RNF	
PRIORIDAD		Nivel de prioridad: ALTA, MEDIA, BAJA.	
CRITERIOS DE ACEPTACIÓN		1. Listado de criterios con los que se pueden cumplir los RNF. 2. …	

[2] Sommerville, Ian. Ingeniería del software. PEARSON-ADDISON WESLEY (2005)

Resultado de Requerimientos.

Al documento de análisis del problema, será actualizado con cambios a descripción y dominio del problema si los hay, para que estos reflejen la nueva sección que se adiciona, la cual corresponde a los requerimientos funcionales y no funcionales. Con este documento se completa la fase de análisis de requerimientos.

Diseño de la Solución de Software

Una vez definidos y validada los requerimientos del sistema, se procede al diseño de la solución informática con el cuál se dará solución. En el diseño de la solución se definen:

- El modelo datos con el diagrama de entidades relaciones (E/R), y el correspondiente diccionario de datos.
- El modelo de la interfaz de usuario.

Modelo de Datos. Diagrama Entidades Relaciones (E/R).

El diagrama E/R es donde se modelan los datos, las relaciones entre las diferentes entidades identificando su cardinalidad. A cada entidad le definimos los atributos que debe poseer, indicando tipo, descripción. Además, se definen llaves primarias y foráneas de cada entidad.

Para facilitar la compresión del modelo de datos, deben de incluirse la descripción de cada modelo, así como la descripción de cada atributo que compone el modelo. Esto con el objetivo de generar un diccionario de datos el cual describa el modelo.

Modelo de la Interfaz del Usuario

La Interfaz de Usuario, en adelante IU, de un programa es un conjunto de elementos que presentan información al usuario y le permiten interactuar para realizar un determinado proceso.

El modelo permite explicar o predecir comportamientos del sistema y tomar las decisiones adecuadas para modificar el mismo. Los modelos subyacen en la interacción del usuario, de ahí su importancia.

El modelado de la interfaz del usuario tiene como objetivo presentar una vista preliminar de cómo se verá la aplicación al usuario, para que este la valide y se puede proceder a dar funcionalidad.

En el modelado se presentan cada una las pantallas enumeradas y además se deberán de indicar cuales de los requerimientos funcionales resuelven, por ejemplo:

Interfaz de Usuario	Casos de Uso
Vista1	**COD01-01**
	COD01-02
Vista2	**COD01-03**
	COD04-01

Resultado: Documento de Diseño.

Al final de esta etapa, se tendrá como resultado el documento de diseño para el problema, el cuál contendrá el modelado de los datos y las interfaces de usuario. Además, el documento de análisis será actualizado con cambios a la descripción del problema y dominio del problema, requerimientos funcionales y no funcionales, para que estos sean un reflejo del documento de diseño.

Desarrollo de la Solución

El desarrollo de la solución consiste en crear la aplicación informática que enlaza la interfaz de usuario con el modelo de datos y los casos de usos (solución al dominio del problema). Para el desarrollo se sigue un marco de trabajo Modelo Vista Controlador (MVC), con el cual nos permite enlazar estos componentes de manera fácil y comprensible. Los modelos son representaciones en código de los modelos de datos; las vistas corresponden a la interfaz de usuario y los controladores implementan toda la lógica de los casos de uso.

Marcos de Trabajo para el Desarrollo de la Aplicación.

Para el desarrollo de las aplicaciones, se usa programación orientada a objetos, con un marco de trabajo MVC: Modelo Vista Controlador. Tenemos tres modelos diferentes de desarrollo dependiendo si se decide utilizar un modelo tradicional web, o un modelo de una sola página, SPA por sus siglas en inglés - Single Page Application. En el caso de SPA, hay variantes de acuerdo a la versión de las herramientas utilizadas:

Modelo Tradicional WEB

- MVC

Modelo una Sola Página:

- MC – MVC
- MC – MVVM

Los marcos de trabajo de una sola página, tienen dos partes, una para el lado del servidor que es donde se implementan los modelos de datos (modelo) y los procesos descritos en los casos de usos (controles). La otra parte de este marco de trabajo se implementa en el cliente y corresponde a la interfaz que mira el usuario (vista), dentro de este se incluye lógica para comunicarse al servidor (controles) enviado la información (modelos) necesaria.

Desarrollo orientado a Módulos.

Para la solución del problema, se desarrolla orientada a módulos, se desarrolla cada uno de los casos de usos y se validan contra el usuario / técnico. Si es necesario se actualizan los documentos de análisis y desarrollo.

Modulo Integrador

Se desarrolla primero el contenedor de toda la solución pensando en los perfiles de usuarios y los accesos que estos deben de poseer, esta parte se deberá de obtener de los casos de usos y los actores. La nueva aplicación y los perfiles se deberán de enlazar a la aplicación ERP para que esta

los administre. Se debe de desarrollar la interfaz (menú) necesaria para enlazar los diferentes interfaces de usuario.

Módulos de la Solución.

Por cada interfaz de usuario, se desarrolla una vista basado en los casos de usos. Se debe de presentar al técnico responsable para su aprobación, de haber cambios, estos deben de modificar los documentos correspondientes. Al terminar la vista correspondiente se procede al siguiente modulo.

Pruebas y Aceptación.

Durante el desarrollo de la solución se deberá llevar una bitácora de actividades, se crea una matriz de desarrollo, la cual deberá de contener por cada caso de uso, la etapa en la que se encuentra, Desarrollo, Pruebas, Aceptación, Solicitud de Modificación, así como una bitácora de acciones implementadas y el historial de observaciones que se presentan.

Interfaz de Usuario	Casos de Uso	Estado	Histórico

Vista1	**COD01-01**	Aceptado	• Acciones realizadas
			  ○ Observación 1
			  ○ Observación 2
			• Acciones realizadas
			• Acciones realizadas
			  ○ Observación 1
			• Documentación

Vista1	**COD01-02**	Desarrollo	• Acciones realizadas • Acciones realizadas
Vista2	**COD02-01**	Pendiente	
Vista3	**COD02-01**	Pendiente	

Guías de Usuario.

Cuando un módulo es aceptado, se procede a la elaboración preliminar del uso de la interfaz de usuario creada. En esta se detallan el proceso que da solución y como se soluciona, se incluye la descripción del modelo de datos. Al final, la documentación deberá de integrarse en un solo documento y se realiza una actualización final, para que la documentación corresponda con los módulos desarrollados. La documentación deberá de ser aprobada por los técnicos encargados del proceso.

Costeo de los sistemas

El cálculo del costo de los sistemas se realizará dependiendo de su forma de producción.

Software adquirido o desarrollado por terceros:

En ese caso el valor del software será el expresado en el contrato, orden de compra, acta de donación o documento equivalente de acuerdo a la cantidad de items involucrados, quedando a cargo de la Jefatura de la Unidad de Desarrollo de Software la valoración de cada uno de los items respecto del monto total en caso de no estar definido previamente.

Software desarrollado con capital humano propio:

Se calculará sobre el total de horas invertidas en el proyecto y el salario del personal asignado al desarrollo del sistema. Para ello, la Jefatura de la Unidad de Desarrollo de Software emitirá un documento formal a la Gerencia de Tecnologías de la Información donde se establezca el valor de acuerdo al criterio antes descrito, para el cual deberá de contener; las horas de trabajo invertidas en las fases de análisis, diseño, desarrollo, capacitación, generación de documento y otras fases que estime convenientes, de acuerdo a lo establecido en la metodología de desarrollo de software institucional hasta la entrega del sistema a la unidad administradora.

Para ninguno de estos casos se tomará en el cálculo de costos el de sistemas operativos de servidores, bases de datos o recursos con los que ya cuente la Institución, sino que solamente deberán incluirse en caso de no contarse previamente por parte de la Institución y sean parte necesaria para el funcionamiento de la solución de software.

Actualizaciones de Software:

Para el cálculo del costo de las actualizaciones, mejoras y mantenimiento de las herramientas de software se utilizarán los mismos criterios establecidos para el desarrollo de software realizado por terceros o con capital humano propio. En el caso de las actualizaciones realizadas con capital humano propio, el costo deberá ajustarse de acuerdo a lo que el marco legal establezca en lo relacionado a la amortización y aumento de valor. Al momento de finalizar una actualización la Jefatura de la Unidad de Desarrollo de Sistemas remitirá a la Gerencia de Tecnologías de la Información un documento donde se establezca el valor de la actualización, para su posterior registro por parte de la Gerencia Financiera de acuerdo a lo establecido en el marco normativo respectivo.

LINEAMIENTO PARA INCORPORAR CAMBIOS A LA BASE DE DATOS EN AMBIENTE DE PRODUCCIÓN

LINEAMIENTO PARA INCORPORAR CAMBIOS A LA BASE DE DATOS EN AMBIENTE DE PRODUCCIÓN

Objetivo

Definir los casos, condiciones y responsabilidades por cambios de contenidos en la Base de Datos cuando están en el ambiente de producción, cuando estos se realicen por medio de programas o aplicativos que no formen parte integral de las aplicaciones informáticas de la CONAMYPE.

Definiciones

- *Base de datos*
  Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación mediante computadora.

- *Aplicación*
  Conjunto de programas con una funcionalidad específica, por ej. ERP de CONAMYPE.

- *Cambios*
  Se refiere a la incorporación, modificación o eliminación de información (contenidos) en la Base de datos en producción con programas diferentes a la aplicación, por alguna de las siguientes causas:
  - Error del Usuario: se origina cuando la persona asignada para operar la aplicación informática de la CONAMYPE realiza un registro incorrecto y la aplicación no tiene un programa u opción para revertirlo o corregirlo.
  - Carga de datos iniciales: Ocurre cuando se instalan aplicaciones nuevas en producción o por actualización o mejora de las aplicaciones ya existentes.
  - Error Generado por fallas en cualquiera de los componentes de la aplicación.

Requisitos Previos

Generación de la modificación en el **Sistema de Gestión de Requerimientos,** adjuntando la Solicitud de cambios en la base de datos en producción (Anexo 1) suscrita y debidamente justificada por Dirección, Gerencia, Jefatura o Coordinación del área responsable de la aplicación en que se originó el error o carga de datos iniciales.

Criterios de Aceptación

Integridad en los contenidos de las Bases de Datos en producción, una vez incorporados los cambios.

Instrucciones Generales

1. La incorporación, modificación o eliminación de contenidos en la Base de Datos en producción, se considerarán como operaciones excepcionales y sujetas a evaluación preliminar por parte de la Gerencia de Tecnologías de la Información.
2. Las Direcciones, Gerencias, Jefaturas y Coordinaciones deberán tomar las medidas pertinentes para evitar la ocurrencia de errores humanos en el registro de la información.
3. La Gerencia de Tecnologías de la Información deberá evaluar y verificar las diferentes opciones de las cuales dispone la aplicación existente para corregir los datos, siempre y cuando estas permitan superar la dificultad.
4. De no ser factible la corrección por los procedimientos que ya estén instalados en la aplicación, la Gerencia de Tecnologías de la Información analizará opciones que superen la dificultad, incorporando o modificando los procesos de la aplicación, elementos de la base de datos, características de la estructura de base de datos y otras, a fin de hacer las correcciones de los datos, así como para incorporar mejoras a dichas aplicaciones.
5. Si se tratara de una aplicación nueva la cual requiriera una carga de datos inicial, estos datos deberán ser certificados por la Gerencia/Unidad responsable de la aplicación, a través del **Sistema de Gestión de Requerimientos**, adjuntando el Formulario Solicitud de Cambios de Contenidos en la Base de Datos en Producción (Anexo 1).
6. Los casos no previstos en estas instrucciones serán resueltos por el Gerente de Tecnologías de Información.

Instrucciones Específicas

Solicitud de incorporación de Modificaciones

1. Las Coordinaciones, Jefaturas, Gerencias o Direcciones que determinen la existencia de un error o inconsistencia en los datos de la aplicación informática en operaciones bajo su responsabilidad, deberán comunicar a través del Formulario Solicitud de Cambios de Contenidos en la Base de Datos en Producción (Anexo 1), adjuntando la documentación que tuviere como evidencia e indicando el inconveniente detectado y la corrección necesaria, esta notificación debe hacerla a través del **Sistema de Gestión de Requerimientos**. Dicha solicitud deberá ser suscrita y debidamente justificada por la persona Responsable de la aplicación.
   En aquellos casos que la Unidad Solicitante requiera que sus técnicos puedan solicitar ajustes a los datos de producción, esta lo podrá realizar delegando aquellas personas que podrán solicitar los cambios mediante memorando suscrito a la Gerencia de Tecnologías de la Información, en el cual justifica su solicitud.

2. Cuando el error en los datos sea generado por mal funcionamiento en los programas, la solicitud deberá ser firmada por La Jefatura de la Unidad de Desarrollo de Software y deberá contar con el visto bueno de la Coordinación, Jefatura, Gerencia o Dirección del Área Responsable de la aplicación.

Evaluación y Viabilidad Técnicas

1. La Gerencia de Tecnologías de la Información al recibir la solicitud, deberá revisar e identificar las causas del error o inconsistencia y evaluar la viabilidad técnica de las correcciones propuestas, a fin de informar a las Coordinaciones, Jefaturas, Gerencias o Direcciones responsables de la aplicación en que se produjo el error o inconsistencia, para que se establezcan tanto las medidas inmediatas a seguir para subsanar el error o inconsistencia; como para establecer en conjunto con la Unidad responsable de la aplicación el plan de trabajo para disminuir o eliminar la probabilidad de ocurrencia del error.

Incorporación de Modificaciones

1. La Gerencia de Tecnologías de la Información a través del Técnico(a) Administrador de Base de Datos, realizará el cambio el cual deberá de ser validado por la Unidad solicitante del mismo, una vez validado el cambio **se cerrará el Requerimiento abierto para el respectivo caso**.

2. Al existir un Requerimiento y este permanece en estado de "esperando retroalimentación" de parte del técnico o Unidad que inicio dicha solicitud; se dará un tiempo prudencial a fin de dar seguimiento a la resolución. Pasado el tiempo prudencial será responsabilidad de la Unidad solicitante la no resolución de la solicitud y será rechazada la asignación del Requerimiento emitido.

Instrucciones Especiales

1. Para efecto de cambios urgentes o de emergencia **en horas hábiles**, se procederá a hacer los cambios de datos, siempre y cuando la no realización del cambio detenga un proceso de atención de un usuario(a), con el compromiso de parte de la estructura solicitando la emisión del Requerimiento a la brevedad posible.

2. En caso de urgencia **en horas no hábiles**, el caso podrá ser generado en el **Sistema de Gestión de Requerimientos**, para efectos de tener la solicitud y acelerar la implementación de la corrección a primera hora del siguiente día hábil, siempre y cuando la no realización del cambio detenga un proceso de atención de un usuario(a).

Para ambos casos, se deberá contar con la autorización de la Dirección, Gerencia, Jefatura o Coordinación responsable de la aplicación y dicha área se compromete a enviar, el día hábil siguiente, la documentación.

Procedimiento para incorporar cambios a base de datos a solicitud de la Unidad de Desarrollo de Software

Cuando la Unidad de Desarrollo de Software necesite realizar ajustes en los procedimientos de las Bases de Datos, primero deberá de realizar el proceso de cambios en el servidor de desarrollo, luego deberá enviar al Técnico Administrador de Base de Datos los script con los cambios a realizar, este verifica los scripts de cambio / creación de estructuras, integridad en la Base de Datos de Desarrollo y procede a realizar el ajuste correspondiente en la Base de Datos de producción, evaluando si el proceso a realizar puede ser optimizado. Previo a realizar el cambio en la Base de Datos del Servidor de Producción, siempre se deberá realizar backup de las Bases de Datos involucradas en el cambio.

POLITICA DE PROTECCION, MANTENIMIENTO, ACTUALIZACIÓN Y SUMINISTRO DE LOS RECURSOS INFORMÁTICOS

POLITICA DE MANTENIMIENTO, ACTUALIZACIÓN Y SUMINISTRO DE LOS RECURSOS INFORMÁTICOS

Objetivo General

El objetivo es regular el suministro, administración, uso, mantenimiento, protección, actualización y la verificación de los recursos informáticos, en aquellas unidades organizativas equipadas y habilitadas con computadoras y demás componentes informáticos de la Institución, así como establecer el mantenimiento preventivo y correctivo del equipo, de tal manera de prolongar hasta el máximo posible, la vida útil de los mismos. Garantizando el cumplimiento de la correcta utilización de los recursos informáticos con los que cuenta la CONAMYPE.

Objetivos Específicos

1. Controlar la calidad en el servicio que se ofrece en la administración de los recursos informáticos.
2. Normar los procesos para el uso eficiente del equipo informático.
3. Cuidar la integridad física del equipo institucional que se encuentra dentro y fuera de las instalaciones de CONAMYPE.
4. Llevar un control del mantenimiento preventivo y correctivo del equipo informático para prolongar su vida útil.
5. Establecer controles administrativos que garanticen la veracidad de las reparaciones, en el servicio del mantenimiento correctivo.
6. Mantener un Sistema de Administración de Software y Hardware.
7. Verificar la correcta utilización de programas y datos.
8. Proveer un marco normativo para la actualización de los equipos informáticos actuales y el suministro de los que sea necesarios.
9. Normar la gestión de los requerimientos realizados a la Gerencia de Tecnologías de la Información.

Alcance

Los recursos informáticos son propiedad de la Comisión Nacional de la Micro y Pequeña Empresa, por lo que su uso es estrictamente institucional. Entiéndase como recursos informáticos todo aquel equipo de computación (Computadoras, Impresores, Equipos de respaldo, etc.), equipos de comunicación (Routers, Modems, AccessPoints, Switches), Programas (Software de Sistemas Operativos, Suites, Antivirus y otros programas) y Sistemas de Aplicación (Bases de datos, Sitios WEB, Intranet).

Definiciones

- *Requerimiento*.

  Para el alcance de esta normativa, se entenderá como requerimiento toda aquella solicitud realizada a la Gerencia, y que sea pertinente al funcionamiento normal de la misma, esto incluye la creación de nuevas funcionalidades de software, reporte de fallas de software o hardware, cambios en la base de datos de producción, etc.

- *Usuarios Autorizados*

  (1) empleados de la Institución;
  (2) otros cuyos accesos complementen la misión de la institución, siempre y cuando su utilización no interfiera con los accesos de otros usuarios a los recursos.

- *VPN*

  Es una red virtual que se crea dentro de otra red real, como puede ser Internet.

PROTECCION DE LOS RECURSOS INFORMATICOS

1. NIVELES DE ACCESO

1.1. USUARIOS

1.1.1. Uso Autorizado

El Uso Autorizado de los recursos informáticos de CONAMYPE será para propósitos relacionados con la misión de la Institución, por lo que el personal deberá limitar su uso al total cumplimiento de sus funciones con el seguimiento de las actividades fundamentales de la institución.

1.1.2. Usuarios Autorizados

Los usuarios y sus niveles de autorización variaran dependiendo del ámbito para el cual se creen. Para el caso de los sistemas informáticos como el ERP, los niveles de autorización y su asignación se realizarán en conjunto con el área administradora del sistema y la Unidad de Desarrollo de Software, de acuerdo a sus procesos internos. En el caso de los servicios como Servicio de Directorios, Servidores, Correo electrónico, y acceso a equipos de infraestructura, será de acuerdo a los niveles que la jefatura de la Unidad de Infraestructura y Seguridad Informática establezca tanto para su operación como para su consulta.

El acceso se otorgará por el jefe(a) de la Unidad de Infraestructura y Seguridad Informática en forma escrita.

2. CUENTAS

2.1.1. Cuentas de acceso

Las cuentas de ingreso a los sistemas informáticos son propiedad de la institución y se usaran exclusivamente para actividades relacionadas con la institución. Ninguna cuenta de usuario autorizado, podrá ser usada para propósitos ilegales, criminales, antiéticos o inmorales.

2.1.2. Tipos de cuentas

Los tipos de cuentas de ingreso de cara al personal en general, son:

- Cuentas de acceso a Dominio.

- Cuenta de acceso a Correo Electrónico.
- Cuenta de acceso a sistema ERP.
- Cuentas de acceso biométrico.

Como parte de las cuentas de ingreso de uso exclusivo del personal de la Gerencia de Tecnologías de la Información se definen:

- Cuentas de administración local a los equipos.
- Cuentas de acceso/administración de servicios externos contratados.
- Cuentas de acceso/administración de servidores o servicios internos.
- Cuentas de acceso/administración de equipos de infraestructura informática y/o telecomunicaciones.

2.1.3. Vigencia de las cuentas

Las cuentas tendrán efecto mientras el usuario mantenga una relación laboral u oficial con la institución. El Jefe(a) de la Unidad de Infraestructura y Seguridad Informática es la única persona autorizada para dar o delegar la creación de accesos a la red.

El personal que el Jefe de esta área organizativa delegue, será el encargado de instalar y configurar los equipos informáticos al nuevo usuario a la red, crear cuentas de domino, correo electrónico y sistema ERP.

2.2. ACCESOS REMOTOS

Ningún usuario podrá realizar accesos remotos a los equipos dentro de CONAMYPE ni desde fuera de la institución, ni desde dentro de la misma, a excepción de aquellos que obtengan la autorización del Jefe(a) de la Unidad de Infraestructura y Seguridad Informática.

2.3. CLAVES DE ACCESO (PASSWORDS)

No se podrá poner claves de Acceso a los equipos informáticos sin previa autorización del Jefe(a) de la Unidad de Infraestructura y Seguridad Informática, tanto al iniciar el equipo (BIOS) o al inicio de sesión en equipos que no sean parte de la estructura de Dominio, ya que es propiedad de la Institución.

Los equipos utilizados para el desarrollo de aplicaciones institucionales en las cuales se encuentra algún código fuente, deberán estar protegidos por claves; estas serán del conocimiento y administración del Jefe(a) de la Unidad de Infraestructura y Seguridad Informática.

El Jefe(a) de la Unidad de Infraestructura y Seguridad Informática, hará cambios periódicos de claves en cuentas de administración de servicios, servidores y equipos para los que no se cuente con un servicio de autenticación vía intercambio de llaves al menos 2 veces al año, para evitar que personas externas puedan tener acceso a los mismos o delegará al responsable de realizar estas tareas.

Las claves de acceso a los servicios internos de la Institución de cara al personal en general que no sean de tipo biométrico deberán ser cambiadas al menos 3 veces al año, y deberán:

- Contener mayúsculas, minúsculas, números y/o caracteres especiales.
- Ser de una longitud de al menos 8 caracteres.

Ningún usuario tendrá rol de administrador en los equipos locales. Sus cuentas serán creadas en el dominio con sus respectivos accesos.

En los casos que las respectivas jefaturas soliciten acceso a la máquina de uno de sus técnicos por ausencia del misma se deberá realizar la solicitud a la Unidad Infraestructura y Seguridad Informática por medios institucionales, quien creará una contraseña temporal para que este pueda acceder y luego deberá ser cambiada por el técnico.

3. PLANES DE CONTINGENCIA GENERALES

3.1 Falla de Energía

Si en horas laborables se corta la energía, es responsabilidad de cada usuario apagar los equipos y las baterías (UPS).

3.2 Respaldo de Servidores y Programas.

Para asegurar la continuidad y el restablecimiento oportuno de los sistemas de información en caso de desastres y cualquier otro evento, la Unidad de Infraestructura y Seguridad Informática deberá implementar una plataforma de respaldos para servidores y bases de datos, garantizando que se generan respaldos al menos una vez a la semana, y que, además, se genera una copia alejada de la ubicación de los servidores.

3.3 Respaldo de las Bases de Datos

Siendo las bases de datos de los activos más valiosos de la institución pues contienen la información transaccional de la institución, a las bases de datos de producción se les deberá de realizar un backup diario, luego el mismo será incremental semanalmente y mensualmente, así mismo el RDBMS central deberá de contar con la redundancia apropiada.

3.4 Respaldo de archivos de usuarios

La Unidad de Infraestructura y Seguridad Informática deberá proveer los servicios y equipos que sean necesarios para el respaldo de la información institucional de los usuarios en servidores destinados para ello, al menos una vez a la semana, para todas aquellas oficinas que cuenten con un servidor de respaldos configurado. En caso de presentarse problemas con la realización periódica del respaldo, el técnico de mantenimiento deberá enviar los respaldos de los usuarios al momento de realizar el mantenimiento preventivo de los equipos.

Los respaldos de archivos de usuarios serán trasladados una vez al año a medios físicos de larga duración, como cintas LTO, y estas serán resguardadas en las oficinas de la Gerencia de Tecnologías de la Información.

El acceso al respaldo de archivos de usuarios deberá ser solicitado vía electrónica o escrita a la Unidad de Infraestructura y Seguridad Informática, el cual brindara acceso de solo lectura a

los datos; dicho acceso será brindado exclusivamente a la jefatura directa en caso que el usuario ya no labore en la Institución, o a quien la Gerencia de Tecnologías de la Información autorice.

3.3 Respaldo al finalizar la relación laboral

Al finalizar la relación laboral con la Institución se realizará un respaldo de todos los equipos informáticos asignados a la persona, y se dejará constancia de la operación a través del formato incluido en el **Anexo 4**.

3.4 Administración de servicios informáticos

La Unidad de Infraestructura y Seguridad Informática será la responsable de garantizar una infraestructura robusta y segura para la implementación de soluciones informáticas, sean estas desarrolladas con software libre o privativo. Como parte de esta infraestructura se incluye la actualización de equipos servidores, equipos de red, sistemas operativos y librerías.

4. PLAN DE CAPACITACIÓN

La Gerencia de Tecnologías de la Información deberá realizar capacitaciones para el uso de las herramientas informáticas puestas a disposición de los usuarios. Para ello podrá hacer uso de capacitaciones presenciales, virtuales, o a través de una solución de gestión del conocimiento que permita el acceso a demanda a recursos de información.

Al momento de la implementación de nuevos sistemas o funcionalidades, la Gerencia de Tecnologías de la Información deberá garantizar que se ha capacitado a todo el personal que tendrá interacción con el sistema.

La Gerencia de Tecnologías de la Información deberá realizar ciclos de capacitación de sus sistemas al menos una vez cada dos años para aquellos usuarios que así lo deseen, así mismo deberá capacitar a los empleados nuevos en el uso de los sistemas en los que estos se encuentren involucrados.

5. MEJORAS Y REVALORIZACIÓN DEL EQUIPO INFORMÁTICO

Para el caso de un equipo informático en el cual reciba una mejora sustancial en sus componentes los mismos deberán de incrementarse su valor y remitirse a la gerencia financiera, el valor a incrementar será el equivalente al suscrito a la orden de compra u contrato, correspondiente a las partes que fueron sustituidas o mejoradas. Para lo cual el Jefe de la Unidad Infraestructura y Seguridad Informática remitirá a la Gerencia de Tecnologías de la Información donde se establezca el valor de acuerdo al criterio antes descrito, con la finalidad de informar a la Gerencia Financiera.

6. IMPLEMENTACIÓN DE NUEVO SOFTWARE

Como parte del proceso de determinación de desarrollo o adquisición de nuevo software, deberá realizarse un estudio a fin de determinar si ya existen soluciones de código abierto que cumplan las necesidades planteadas. En caso que exista una solución que cumpla con el estándar de código abierto, y que además cumpla los siguientes criterios:

- Tener más de 2 años de existir.

- Demostrar soporte continuo, ya sea de sus creadores o la comunidad, debiendo tener un nuevo reléase, ya sea de desarrollo o mantenimiento en los 4 meses previos al estudio.

Se podrán implementar tecnologías que no cumplan los requisitos previos, siempre que se haga de manera experimental, en ambientes controlados, para mantener un enfoque de mejora continua en el área de tecnologías.

De la misma manera, se podrá adquirir software propietario por encima de una solución de código abierto para aquellos servicios críticos, tales como infraestructura, servidores (físicos o virtuales),bases de datos, herramientas para desarrollo de software u otras que por su naturaleza requieran soporte directo y de primera línea con el fabricante, para lo anterior la Jefatura de la Unidad de Infraestructura y Seguridad Informática así como la Jefatura de la Unidad de Desarrollo de software deberá de realizar el estudio apropiado enviándolo a la Gerencia de Tecnologías de la Información para su aprobación . Esto con el fin de mantener un entorno seguro y estable para el funcionamiento y resguardo de los activos tecnológicos de la Institución.

Cuando se esté por adquirir software propietario se deberá favorecer aquellas soluciones que obtengan la calidad de líderes en el cuadrante de gartner a la fecha de su adquisición.

GESTION DE REQUERIMIENTOS DE USUARIOS

Todo requerimiento realizado a la Gerencia de Tecnologías de la Información deberá realizarse vía Sistema de Gestión de Requerimientos. Todo requerimiento deberá incluir un detalle de situación, y los archivos adjuntos que el solicitante considere necesario. Para facilitar el trabajo en situaciones de emergencia, si el requerimiento se recibe de emergencia o vía telefónica, podrá ingresar el requerimiento en lugar del usuario.

Los requerimientos serán distribuidos al personal correspondiente por parte de su jefatura para evaluar factibilidad, y procedencia del requerimiento. De no encontrarse factible o procedente, se procederá al rechazo del mismo.

El personal técnico procederá con la resolución del requerimiento, y de faltar información o ser necesaria aclaración al respecto, solicitará retroalimentación al usuario. Al realizar cualquier acción o resolver el requerimiento, el técnico asignado deberá dejar constancia de las acciones realizadas.

Un requerimiento en espera de retroalimentación no puede pasar permanentemente en ese estado, por lo tanto, se dará un tiempo prudencial para que el usuario pueda ingresar la información solicitada, el cual será de 15 días calendario. Al pasar dicho periodo de tiempo se dará por resuelto el requerimiento, y el usuario deberá ingresar uno nuevo, si bien puede hacer referencia al requerimiento resuelto.

ADMINISTRACION DE SOFTWARE

LICENCIAS

La Unidad de Infraestructura y Seguridad Informática mantendrá un inventario de productos de software con licencia, instalados equipos informáticos institucionales, con el objetivo de estandarizar, retirar equipo obsoleto, evaluar el uso y revisar procedimientos.

Se tendrá un control de licencias y un control por tipo de licencias.

La institución se reserva el derecho de rehusarse a defender a cualquier empleado ante cualquier asunto legal relacionado a infracciones a las leyes de protección de la propiedad intelectual. Por lo que queda prohibido para el personal en general instalar software, que no sea autorizado por el Gerente de Tecnologías de la Información.

La Gerencia de Tecnologías de la Información deberá dar visto bueno a cualquier solicitud de adquisición de Hardware y/o Software que realicen el personal de CONAMYPE, ya sea por mantenimiento, actualización o ampliación del equipo informático o software de la institución.

PROPIEDAD INTELECTUAL

La institución mantiene la propiedad sobre toda la información técnica y administrativa creada o modificada por sus empleados como parte de sus funciones laborales.

DESARROLLO DE SOFTWARE.

Todas las aplicaciones que se desarrollen para la CONAMYPE deben contar con pistas de auditoria a través de bitácoras electrónicas contenidas en todos los sistemas, que permitan verificar la correcta utilización de los programas y de los datos.

ADMINISTRACION DE HARDWARE

MANTENIMIENTO PREVENTIVO DE EQUIPO INFORMATICO.

El Mantenimiento preventivo del equipo informático, así como cualquier modificación o ampliación de nuevos puntos de red de datos, actualizaciones y reparaciones será financiado por la institución.

Las operaciones de mantenimiento del equipo informático tienen prioridad sobre el uso ordinario que de la misma hagan los usuarios.

El Jefe(a) de la Unidad de Infraestructura y Seguridad Informática comunicará en forma escrita o por correo electrónico, la programación del mantenimiento preventivo a los usuarios.

MANTENIMIENTO CORRECTIVO DE EQUIPO INFORMÁTICO

Será responsabilidad del usuario reportar la falla que tiene el equipo, mediante un requerimiento en el Sistema de Gestión de Requerimientos, el cual es parte del ERP.

El Jefe(a) de la Unidad de Infraestructura y Seguridad Informática dará el visto bueno de la solicitud de compra de repuestos cuando así lo amerite el reporte de la falla, y se determine que el daño en el equipo no sea responsabilidad del uso indebido del equipo por parte del usuario, en cuyo caso se remitirá el caso al encargado de activo fijo para el proceso respectivo.

El Jefe(a) de la Unidad de Infraestructura y Seguridad Informática o quien este delegue controlará mediante formulario el equipo de computación que salga de la institución por motivos de reparación, enviándole una copia al encargado de activo fijo para su conocimiento.

REEMPLAZO DE EQUIPO INFORMATICO

El equipo informático será sustituido o retirado en un periodo de entre 3 y 5 años, cuando pierda su vida función, su costo de reparación sea mayor al de su valor actual, o se encuentre dañado de forma irreparable. Esto con el fin de prevenir cualquier tipo de daño a la información que se pueda ocasionar por tener un equipo desfasado, o costos excesivos de reparación.

Cuando sea necesario el descarte del activo, se presentará el detalle a la Dirección de Tecnología e Innovación y con el visto bueno de la Gerencia de Tecnologías de la Información a fin que este sea presentado ante la Presidencia o la Junta Directiva según corresponda para el trámite correspondiente.

NORMAS PARA USO DEL EQUIPO DE COMPUTACION

1.0 DISPOSICIONES GENERALES

Los usuarios de los recursos informáticos están obligados a:

a) Cumplir con lo dispuesto en la normativa para uso de los recursos informáticos.

b) Cumplir con la sección 2.0 de Antivirus de este romano.

c) Prestar su colaboración al personal encargado de hacer los mantenimientos de los recursos informáticos.

d) Atender las contingencias en caso de corte de energía, caída de señal de Internet, averías en los equipos; y notificar de lo sucedido a personal de la Unidad de Infraestructura y Seguridad Informática.

e) Reportar a la Unidad de Infraestructura y Seguridad Informática, vía Requerimiento en sistema, cualquier falla o irregularidad detectada en su equipo.

f) No modificar las configuraciones de los equipos de cómputo.

g) No mover el equipo informático de una unidad organizativa a otra, sin previa aprobación de la Gerencia de Tecnologías de la Información, mediante formulario de traslado de activo fijo generando una copia al encargado de activo fijo de la Institución.

h) Hacer uso racional, eficiente y considerado de los recursos disponibles tales como: Internet, Correo electrónico, el espacio en disco y periféricos (Impresores, Respaldos, Scanner y el mismo computador asignado)

i) No deberá de utilizar ninguna información de la institución para uso personal.

j) No deberá copiar a memorias USB, CD o DVD información institucional con fines ajenos al desarrollo de la misma.

k) No modificar en ninguna manera el exterior de los equipos. Esto incluye, pero no se limita a: viñetas adhesivas, magnetos, etc. Tampoco deberá remover cualquier tipo de identificación institucional del mismo.

l) No permitir la modificación o reparación de equipos por parte de terceros. La reparación o tercerización de la reparación es una atribución exclusiva de la Gerencia de Tecnologías de la Información.

2.0 ANTIVIRUS

Para seguridad de todos los usuarios de la red local, se deberá observar las siguientes reglas mínimas para evitar o minimizar daños causados por virus de computadora:

a) No abrir archivos ejecutables que llegan desde algún lugar desconocido o no confiable, por ejemplo, archivos que tienen la extensión .EXE, .BAT, COM, .PIF o. SHS. No importa si los archivos llegan por medio de una USB, un correo electrónico, descarga de internet, etc.

b) Abstenerse de enviar o reenviar mensajes conteniendo archivos como los arriba indicados.

c) Cuando el programa anti-virus instalado detecta algún virus en la computadora, deberá borrarlo, y no repararlo.

d) Después de detectar y borrar un programa infectado, deberá apagar la computadora y volver a encenderla, para eliminar cualquier rastro de virus en memoria.

e) Verificar memorias USB con el antivirus, antes de utilizarlo en su computadora.

f) Si no se acatan estas recomendaciones será responsabilidad del personal, el que el equipo asignado sufra un problema irreparable por causa de virus y por reclamos de terceros por la misma causa.

Normativa relacionada

- Lineamiento para incorporar cambios a la base de datos en ambiente de producción.
- Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público de la Corte de Cuentas de La República.

POLÍTICA DE INFRAESTRUCTURA DE LLAVE PÚBLICA Y FIRMA ELECTRÓNICA SIMPLE.

POLÍTICAS DE INFRAESTRUCTURA DE LLAVE PÚBLICA Y FIRMA ELECTRÓNICA SIMPLE.

Antecedentes

La necesidad de una política que detalle la estructura de llave publica es primordial para la implementación de la firma electrónica simple y sus distintas aplicaciones, de manera que cumpla los requerimientos establecidos en la Ley de Firma Electrónica, la Ley de Procedimientos Administrativos y la normativa de la Corte de Cuentas de la Republica.

Objetivo

Delimitar los requerimientos, roles y funciones a establecerse con la Infraestructura de llave publica de la CONAMYPE.

Desarrollo

La infraestructura de llave publica de la Comisión Nacional de la Micro y Pequeña Empresa deberá proveer los equipos servidores, procedimientos y herramientas para garantizar:

- Autenticidad, con el cual se garantiza que el mensaje es confiable y esta garantía perdura a través del tiempo;
- Integridad, por el cual se otorga certeza que los datos recibidos por medios electrónicos no han sido modificados en su tránsito, desde el iniciador hasta el destinatario;
- Confidencialidad, por medio del cual se garantiza al iniciador y destinatario, que los mensajes electrónicos no serán conocidos por terceras personas, sin su expresa autorización;
- No Repudiación, por medio del cual se garantiza que cuando un mensaje ha sido suscrito con firma electrónica, no puede ser repudiada su autoría por la persona del iniciador;

Para ello, la Gerencia de Tecnologías de Información a través de la Unidad de Infraestructura y Seguridad Informática proveerán de las herramientas de hardware y software necesarias para el montaje de una PKI.

Siempre se deberá contar con al menos tres servidores que servirán como Autoridades Certificadoras:

- Uno como Certificadora Raíz.
- Uno como Certificadora Intermediaria
- Uno como Certificadora de Identidades

Adicionalmente, se deberán implementar servidores que provean los siguientes servicios:

- Uno o más servidores de validación de firmas OCSP. Pueden ser procesos individuales para cada CA en un solo servidor.
- Servidor de Sellado de Tiempo o TSA para el proceso de firma electrónica de documentos.

Todos los servidores que forman parte de la PKI deberán cumplir con los siguientes requisitos de seguridad:

- Cumplir con la política de cambio de contraseña de la CONAMYPE, realizando cambios de contraseña cada dos meses para los usuarios sin privilegios administrativos.
- La autenticación de usuarios vía SSH será únicamente con llave pública. La autenticación con contraseña deberá estar deshabilitada, y el usuario root no podrá iniciar sesión vía SSH.
- Tener habilitados únicamente los puertos necesarios para administración vía SSH, puertos especificados para OCSP, y conexión de unidades remotas vía NFS o SMB.

En términos de funcionamiento, la PKI se inicializará de la siguiente manera:

1. Se generará el primer par de llaves para la certificadora raíz. La generación de este par de llaves se dará de acuerdo el procedimiento establecido en este documento.
2. Se generará el certificado de la CA Raíz.
3. Se generarán las llaves y solicitud de certificado de la entidad CA Intermediaria.
4. Se firmará la solicitud de certificado de la CA intermediaria por parte de la CA Raíz.
5. Se trasladará dicho certificado y llaves a la CA Intermediaria.
6. Se apagará el servidor que hace las veces de CA Raíz, a fin de separarlo por completo de ataques que pudieran comprometer la integridad de la PKI.

Luego de realizado este procedimiento, se trabajará con la CA intermediaria para la generación de certificados para otras CA, como es el caso de la CA de Identidades, de acuerdo al Proceso de Generación de Certificados para Autoridades de Certificación.

Procedimiento de Generación de Certificado para Entidad Certificadora Raíz

1. Se inicia sesión en el equipo que fungirá como Certificadora Raíz. Previo al inicio de este proceso se deberá contar con la presencia del Director de Innovación y Tecnologías, un representante de la Unidad de Auditoria Interna institucional y un representante de la Unidad Legal Institucional.
2. El Director de Innovación y Tecnologías ingresa una clave que estará relacionada a la llave privada de la CA Raíz. El director deberá guardar esta clave en papel, guardarla en un sobre sellado, y este sobre deberá dársele el resguardo correspondiente, siendo bóveda la preferencia.
3. El personal de la Gerencia de Tecnologías de la Información iniciara la creación del certificado de la CA, y el Director de Innovación y Tecnologías ingresara la clave secreta previamente creada.
4. Se repetirá el proceso para la firma del certificado de la CA intermedia.
5. Se levantará acta de la realización de este procedimiento, y el original será guardada por la Dirección de Innovación y Tecnología.

Proceso de Generación de Certificados para Autoridades de Certificación

1. Se genera el par de llaves en servidor que fungirá como CA.
2. Se genera la solicitud de certificado.
3. Se traslada dicha solicitud de certificado a la CA superior, la cual agrega su certificado a la cadena y aprueba el certificado.
4. El certificado es transferido al servidor solicitante, que se transforma en CA.
5. Se usa el certificado para la acreditación propia y generación de certificados que dependan de esta CA.

Para el caso de las personas trabajadoras de la Institución se generarán sus llaves y certificados siguiendo el Proceso de Generación de Certificados para Empleados de la CONAMYPE, y su revocación en el Proceso de Revocación de Certificados para Empleados de la CONAMYPE.

Características de los certificados de Empleado

- Su uso e instalación están relacionados a una clave provista por el empleado.
- Tendrán una vigencia de 5 años.
- Su uso esta exclusivamente relacionado a los documentos de uso interno, de acuerdo a las limitantes establecidas en la Ley de Firma Electrónica.

Proceso de Generación de Certificados para Empleados de la CONAMYPE.

1. El empleado deberá presentarse en persona a las oficinas de la Unidad de Infraestructura y Seguridad Informática, mostrando su carnet de empleado para identificarse.
2. El personal designado en la Unidad iniciara el proceso de llenado de la solicitud de certificado, solicitando los siguientes datos:
    a. Nombre completo del empleado
    b. Usuario de correo electrónico
    c. Unidad Organizativa a la que pertenece el empleado
    d. Nombre de la Oficina en la que esta destacado.
    e. Departamento en que se encuentra la Oficina en que esta destacado.
3. Para la creación de la contraseña de la llave privada del empleado, este deberá ingresarlo personalmente, y luego reingresarla para garantizar su exactitud.
4. El personal designado presentara los datos del certificado a punto de ser registrado en la CA de Identidades, y los registrara previa validación por parte del empleado.
5. Se descargará y entregará el certificado digital recién emitido al empleado únicamente vía dispositivo de almacenamiento masivo extraíble, nunca por correo electrónico ni a terceros.

Proceso de Reemisión de certificado

Este proceso puede darse por diversas razones, no limitándose al olvido de clave del certificado por parte del usuario o por la expiración del mismo. El proceso a seguir es el siguiente:

1. La persona empleada informa a la Unidad de Infraestructura y Seguridad Informática ya sea por teléfono, requerimiento o correo electrónico de la situación.

2. El personal de la UIS realiza el proceso de Revocación de Certificados para Empleados de la CONAMYPE.

3. La persona empleada se hace presente a las oficinas de la UIS para seguir el proceso de Generación de Certificados para Empleados de la CONAMYPE.

Proceso de Revocación de Certificados para Empleados de la CONAMYPE.

1. La Unidad de Infraestructura y Seguridad Informática es notificada de la solicitud de revocación por las siguientes causas y personas:
    a. Olvido de clave de la llave privada: Empleado afectado.
    b. Vencimiento del certificado: Empleado afectado.
    c. Cese de relación laboral con el empleado: Gerencia de Talento Humano.
2. El personal de la Unidad procede a revocar el certificado del empleado relacionado.

Uso de firma electrónica en documentos generados vía sistemas informáticos.

Para que un sistema informático haga uso seguro de la funcionalidad de firma electrónica para un empleado deberá cumplir los siguientes requisitos:

- Creación de una API que permita la interacción segura con el almacén de llaves privadas.

- Las llaves privadas jamás deben salir de su almacén de datos. Toda solicitud de firma se dará programáticamente proveyendo el identificador de usuario y la clave.

- Toda comunicación entre servidores y aplicativos debe darse usando protocolos seguros de comunicación como HTTPS.

Los documentos firmados digitalmente por un empleado a través de un sistema informático deberán ser almacenados de manera segura en un almacén de datos designado para ello, y deberán ser resguardados de acuerdo a lo establecido por Ley.

Definiciones

- *PKI*

  Public Key Infrastructure o PKI por sus siglas en inglés, es la infraestructura de llave pública, y es el sistema requerido para proveer cifrado de llave pública y servicios de firma digital.

- *CA*

  Certificate Authority o CA por sus siglas en inglés, es como se nombra a una Autoridad Certificadora. Representan las personas, procesos y herramientas para vincular los nombres e información de las entidades usuarias a sus llaves públicas. Al crear certificados las CA actúan como agentes de confianza dentro de la PKI.

- *Llave publica*

  Llave criptográfica que puede ser obtenida por cualquiera para encriptar mensajes dirigidos a un destinatario particular, de manera que el mensaje cifrado puede ser únicamente descifrado usando una segunda llave conocida por el destinatario (llave privada)

- *Llave privada*

  Llave criptográfica que no debe ser compartida con nadie, y sirve para descifrar mensajes dirigidos hacia su poseedor. Dichos mensajes debieron haber sido cifrados con la llave pública relacionada.

- *TSA*

  Timestamp Authority o TSA por sus siglas en inglés, representa las personas, procesos o herramientas para marcar inequívocamente la fecha y hora en que un documento es firmado digitalmente.

- *OCSP*

  Online Certificate Status Protocol o OCSP por sus siglas en inglés, es el protocolo diseñado para la revisión de estado (validez) de un certificado digital.

- *UIS*

  Unidad de Infraestructura y Seguridad Informática de la CONAMYPE.

Normativa Relacionada

- Ley de Firma electrónica
- Ley de Procedimientos Administrativos

POLÍTICA DE SEGURIDAD FÍSICA Y LÓGICA PARA LOS CENTROS DE DATOS INSTITUCIONALES

POLÍTICA DE SEGURIDAD FISICA Y LÓGICA PARA LOS CENTROS DE DATOS INSTITUCIONALES.

Objetivo

Brindar el marco normativo aplicable para reducir los riesgos de seguridad para los centros de datos institucionales, tanto lógica como físicamente.

Objetivos específicos

- Proveer los lineamientos para la seguridad física y lógica de los centros de datos que se encuentren en las instalaciones de la Institución.
- Proveer los lineamientos para la seguridad física y lógica de los centros de datos que se encuentren en sitios externos.

Definiciones

- *UISI*

  Unidad de Infraestructura y Seguridad Informática

- *Disponibilidad*

  Cuando se usa respecto a centros de datos, hace referencia a la capacidad del mismo para proveer servicios sin interrupción a sus usuarios.

- *ANSI-TIA-942*

  Estándar de la Asociación de la Industria de las Telecomunicaciones - Telecomunication Industry Association en inglés-, incluye una serie de especificaciones para comunicaciones y cableado estructurado y subsistemas de infraestructura, proveyendo además formas de clasificar estos subsistemas.

- *Cortafuegos*

  Parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- *Zona desmilitarizada*

  En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

- *SSH*

  Secure Shell es un protocolo y programa que cuya principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada.

- *SFTP*

  SSH File Transfer Protocol, permite una serie de operaciones sobre archivos remotos.

- HTTPS

  Protocolo seguro de transferencia de hipertexto (en inglés, Hypertext Transfer Protocol Secure o HTTPS) es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto.

Desarrollo

La Gerencia de Tecnologías de la Información, a través de la Unidad de Infraestructura y Seguridad Informática será responsable de dar cumplimiento a los siguientes criterios de seguridad física y lógica a fin de resguardar de la mejor manera los datos y servicios institucionales, junto a su infraestructura lógica.

Seguridad física de los centros de datos institucionales internos

Tomando como base los riesgos identificados y previstos en el plan de contingencia informática, los centros de datos institucionales internos deberán contar con las siguientes medidas de seguridad física:

- Acceso controlado

  El acceso a los centros de datos será estrictamente prohibido para personal no relacionado al área. El personal que no sea parte de la Institución que deba por razones de trabajo realizar acciones en el centro de datos, deberá estar acompañado por personal de la UISI.

- Monitoreo de actividades

  Las actividades realizadas dentro del centro de datos deberán ser monitoreadas las 24 horas del día, de manera que se documente cualquier situación que pueda darse.

- Medidas contra incendios

  El centro de datos deberá contar con sistemas contra incendios que monitoreen activamente el centro de datos, y que se activen de forma automática de ser necesario, sin implicar que el uso del agente extintor dañe los equipos.

- Gabinetes cerrados

  Todos los gabinetes del centro de datos deberán poseer cerraduras frontales y posteriores, que permitan asegurar el resguardo de los equipos instalados.

De la misma manera, todos los equipos servidores que posean carátulas frontales deberán portar las mismas aseguradas.

Seguridad física de los centros de datos institucionales en sitios externos

Los proveedores de servicios de alojamiento para los servidores institucionales deberán garantizar además de las condiciones establecidas para los centros de datos internos:

- Nivel de disponibilidad

El proveedor deberá garantizar que el centro de datos cumpla al menos con la especificación técnica ANSI-TIA-942 de nivel o Tier II.

Seguridad lógica de los centros de datos institucionales

Cada centro de datos institucional deberá poseer al menos las siguientes medidas de seguridad lógica:

- Separación de Red

Los servidores y sus máquinas virtuales deberán estar separados de la red de clientes, en una red de área local, ya sea virtual (vLAN) o física (LAN) exclusiva. No deberá permitirse la asignación de direcciones a usuarios finales dentro de esa red.

- Cortafuegos perimetrales

Deberá implementarse un cortafuegos o firewall perimetral que separe la red de servidores de las otras redes. De la misma manera, deberá proveer herramientas de análisis de paquetes y análisis de tráfico para detección temprana de amenazas.

Cada servidor deberá exponer solamente los puertos que sean estrictamente necesarios para el consumo de sus servicios a través del firewall.

- Zona desmilitarizada

De ser necesaria la utilización de una zona desmilitarizada (DMZ), esta podrá ser implementada de manera virtual, siempre y cuando se respeten los principios de funcionamiento de esta zona, es decir, una LAN separada y expuesta de manera pública.

- Accesos lógicos

El acceso administrativo a los servidores y sus máquinas virtuales deberá realizarse por protocolos seguros como SSH, SFTP y HTTPS. En ese sentido, protocolos inseguros como TELNET no estarán habilitados en los mismos, a menos que sea estrictamente necesario para el funcionamiento de una

aplicación, para lo cual se deberán implementar las medidas de seguridad que compensen la exposición al riesgo.

De la misma manera, el acceso del superusuario estará deshabilitado de manera remota sin excepción.

- Longitud y vigencia de las contraseñas

En todos los servidores donde sea posible, el acceso vía terminal remota se deberá implementar a través de SSH versión 2 o superior, y haciendo uso de autenticación con intercambio de llaves.

En los casos donde lo anterior no sea posible, y deban usarse contraseñas, las siguientes consideraciones son de carácter obligatorio:

  - Las contraseñas deberán tener una longitud de 12 caracteres o más, incluyendo mayúsculas, minúsculas, números y símbolos.
  - Las contraseñas no deberán compartirse con personal fuera de la Gerencia.
  - Las contraseñas deberán cambiarse periódicamente, al menos cada 6 meses.

Normativa Relacionada

Normas Técnicas de Control Interno de la Comisión Nacional de la Micro y Pequeña Empresa.

POLÍTICAS DE USO DE INTERNET Y CORREO ELECTRÓNICO.

POLÍTICAS DE USO DE INTERNET Y CORREO ELECTRÓNICO

Objetivo.

Regular y controlar los componentes y servicios relacionados con el uso de Internet y Correo Electrónico; para proteger la información, así como la confidencialidad de la misma.

Alcance.

Las políticas para uso de Internet y Correo Electrónico, será aplicable a todos los funcionarios y empleados de la CONAMYPE, sin excepción; así como, a todas las empresas y terceros que reciban este beneficio y que lo utilicen para realizar actividades laborales autorizadas.

Debe entenderse, que la norma es aplicable a todos los casos en los cuales la CONAMYPE y/o los funcionarios y empleados de la misma, hayan efectuado directa o indirectamente una conexión a redes locales, remotas, públicas, privadas o de cualquier otra índole.

Restricciones y Derechos.

Los medios de conexión e instalación de internet y correo electrónico que la institución proporciona a sus funcionarios o empleados, son propiedad de la CONAMYPE. Se da por entendido que se brindan dichos servicios única y exclusivamente como una herramienta de trabajo, y que, por tanto, su uso deberá ser explícitamente en materias relacionadas al cargo que desempeña. Si bien puede hacerse uso personal del acceso a internet en horas de descanso, este debe ser un uso moderado para no causar afectación a los servicios de la Institución.

Con el objeto de establecer y garantizar el cumplimiento de estas normas, la CONAMYPE realiza las siguientes acciones:

- Controlar el uso laboral o personal de los medios de conexión a Internet.
- Recolección, almacenamiento y registro de información referente a los sitios visitados en Internet a través de sus enlaces.
- Suspender temporal, parcial o definitivamente la conexión e instalación de internet o correo electrónico provisto a los funcionarios o empleados, debido a un mal uso del medio provisto.

Definiciones.

- *Acceso Remoto.*

  Ingresar a la red de la CONAMYPE desde una computadora que no pertenece física o lógicamente a la Red de datos de la institución, que necesita equipo de comunicación para realizar la conexión.

- *Solicitud de Entrega de Correo.*

  Un tipo de mensaje que se envía para indicar que un bloque de datos ha llegado a su destino sin errores.

- *Ancho de Banda.*

  Se refiere a la capacidad de transmisión de un canal de comunicación. Indica la cantidad de información por unidad de tiempo que puede enviarse a través de una línea de transmisión, medida frecuentemente en bits por segundos (bps).

- *Cadena de Comunicación.*

  Una guía que nos ayuda a transmitir adecuadamente a un superior, una petición para aclarar o resolver situaciones laborales.

- *Clientes*

  Es toda aquella persona que hace uso de los recursos de internet o correo electrónico de CONAMYPE.

- *Conexiones remotas.*

  Operación realizada en una computadora, a través de internet o de una red local.

- *GTI*

  Gerencia de Tecnologías de la Información.

- *Encriptar.*

  Codificar un mensaje o texto con software especializado a fin de proteger información. El resultado de encriptar un correo o archivo es que no puede ser visualizado normalmente a menos que el receptor posea el software con el cual se encriptó el mensaje de correo o archivo de texto y, además, debe poseer una llave lógica que le autoriza a visualizarlo en forma normal.

- *Internet*

  Debemos entender que, al mencionar internet, se incluyen implícitamente, todos los servicios inherentes a este servicio, tales como: Mensajería Instantánea, Buscadores, Correo Electrónico, Redes Sociales, Carga, Descarga, etc.

- *Derechos de Autor.*

  Son leyes que protegen a los creadores, autores o propietarios de la reproducción, distribución o venta ilegal de sus creaciones.

- *Licencia.*

  Es un documento escrito en papel o electrónicamente que da derecho a un ente a usar de acuerdo a los términos de la misma, software o programas.

- *Mensajería instantánea*

  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.

- *Medios de conexión.*

  Son los dispositivos físicos, técnicas, forma de transmisión de datos y programas que se utilizan para tener comunicación y acceso a internet y al correo electrónico.

- *Navegador Web*

  Es una aplicación que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente escritos desde servidores Web de todo el mundo a través de internet. Los navegadores actuales pueden ejecutar: gráficos, secuencias de video, sonido, animaciones y programas diversos, además hipervínculos o enlaces.

- *Política.*

  Acción de carácter administrativo tendiente a regular y controlar el uso de recursos propiedad de la CONAMYPE, para disminuir los riesgos de uso inadecuado de los mismos.

- *Red.*

  Conjunto de computadoras y otros equipos de cómputo, agrupados y distribuidos bajo ciertos criterios alrededor de uno o varios Servidores, con el objeto de compartir, almacenar o intercambiar información. Los grupos de computadoras y equipos de cómputo pueden estar ubicados en un mismo o en diferentes sitios y pueden o no permitir el acceso de usuarios locales o remotos.

- *Seguridad lógica*

  Se refiere a la certeza en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

- *Servidor.*

  Son computadoras de alto rendimiento, con alta velocidad de procesamiento y gran capacidad de almacenamiento, utilizadas como repositorios de datos, programas y aplicaciones, cuyo objetivo fundamental es dar atención al resto de computadoras personales y estaciones de trabajo de una o más redes.

- *Sistemas.*

  Se refiere a la red de la CONAMYPE, más un conjunto de programas de software, aplicaciones, programas, personal a cargo de su gestión y equipos de comunicación propiedad de la institución.

- *SPAM.*

  Son mensajes electrónicos (habitualmente de tipo comercial o promocional) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general, es la basada en el correo electrónico no deseado.

- *Tráfico en la red.*

  Cantidad de datos enviados a través de internet por un equipo cliente.

- *Usuarios*

  Funcionario o empleado que utiliza los servicios informáticos.

- *Malware*

  También conocidos anteriormente como virus informáticos, son herramientas de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. Estos pueden presentar las características siguientes:

  - Se reproducen o replican a sí mismos y se propagan a otras computadoras.
  - Se insertan o afectan los programas ejecutables, cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador vaya a ejecutar.
  - Se cargan a la memoria del computador pudiendo reproducirse y copiarse en medio de almacenamiento y/o software instalado en el disco duro.
  - Infectan las computadoras a través de ficheros enviados conjuntamente con los mensajes.
  - Pueden alterar, destruir o borrar la información contenida en las computadoras.

1. Normas.

1.1 Autorización.

1.1.1 Para obtener acceso a internet y correo electrónico, a efecto de realizar actividades laborales, en forma temporal o permanente, debe ser autorizado por el Jefe Inmediato de la Unidad Organizativa, quien tramitará por medio del formulario FDDI001 Solicitud de Autorización para Conexión a Internet y Correo Electrónico, para la instalación del servicio (Anexo 1).

Asimismo, el jefe o superior jerárquico solicitará cuando sea necesario o lo considere pertinente la desinstalación de los mencionados servicios.

1.1.2 Si el empleado es trasladado de una unidad a otra, se le inactivarán los accesos y se deberá tramitar nuevamente la autorización para el uso de los recursos.

1.2 Utilización de internet.

1.2.1 Los usuarios que tengan acceso a internet y correo electrónico, harán uso de los mismos para fines del cumplimiento de sus labores institucionales.

1.2.2 En caso de ser necesaria la conexión de otros dispositivos para conectarse a Internet (modem USB, teléfonos celulares, etc.), su autorización deberá solicitarse al Unidad de Informática (UI) por el Jefe de la Unidad Organizativa previa justificación del caso, a través del formulario

FDDI002 Solicitud de Autorización para Conexión a Internet por medio de modem inalámbrico (Anexo 2).

1.2.3 La información contenida en las computadoras y los mensajes de correo electrónico no podrán reproducirse o utilizarse para fines ajenos a las funciones de la CONAMYPE, debido a que la información es de propiedad intelectual de la misma.

1.2.4 La cuenta de red y correo electrónico es personal, intransferible e irrenunciable, asimismo, obliga a cada usuario a aceptar las normas establecidas por la Institución y a someterse a ellas.

1.2.5 Todas las conexiones realizadas a Internet y correo electrónico serán monitoreadas y registradas por medio de software especializado.

1.2.6 Toda actividad que vaya en contra de esta normativa será reportada a su jefe inmediato o autoridad competente, por medio de la jefatura de la Unidad de Infraestructura y Seguridad Informática.

1.2.7 Se bloquearán descargas de páginas o de archivos, y todas aquellas que puedan ocasionar una distorsión en el servicio de internet, es decir, uso excesivo del ancho de banda por periodos extendidos de tiempo. Como, por ejemplo: Radio por internet, descarga de videos o música, protocolos de transferencia de archivos p2p, etc.

1.2.8 Toda actividad realizada con el servicio de internet, es responsabilidad del usuario propietario de la cuenta utilizada.

1.2.9 Los usuarios del servicio de internet, no deben generar ningún mensaje o publicación que contenga ataques escritos, amenazas a otros usuarios u organizaciones, o mensajes cuya intención sea acosar, molestar o alarmar a otras personas.

1.2.10 Se presentará un reporte trimestral de uso de internet de todas aquellas personas que utilicen de manera excesiva el servicio y no justificada.

1.2.11 La Gerencia de Tecnologías de la Información podrá restringir paginas para los empleados sin previo aviso, debiendo informar a la Dirección de Calidad Innovación y Tecnología sobre las razones de su restricción.

1.3 Conexión a Internet y Acceso Remoto a Redes y Sistemas.

1.3.1 La conexión a internet institucional debe realizarse en redes que pertenecen a la CONAMYPE y únicamente puede ser configurada por un técnico autorizado de la Gerencia de Tecnologías de la Información.

1.3.2 Toda la actividad del tráfico entrante o saliente a Internet de la institución, debe atravesar los dispositivos de seguridad establecido por la Gerencia de Tecnologías de la Información para que se puedan aplicar los controles de acceso y los demás mecanismos de seguridad. Las excepciones a esto deben ser autorizadas por el Gerente de Tecnologías de la Información, previa solicitud y análisis del mismo.

1.3.3 Los usuarios no deben probar o sondear los mecanismos de seguridad en la institución o en otros sitios de Internet a menos que hayan obtenido un permiso por escrito por parte de la Gerencia de Tecnologías de la Información.

1.3.4 La posesión o el uso de herramientas para detectar los aspectos vulnerables de los sistemas de información o para comprometer los mecanismos de seguridad de la información, se considerará una falta grave y dará lugar a las sanciones correspondientes, todo acceso deberá de tener autorización por parte de la Gerencia de Tecnologías de la Información.

1.4 Intercepción de Material Confidencial

1.4.1 La CONAMYPE puede intercambiar o requerir información confidencial de sus clientes; por ello el comportamiento de los usuarios y técnicos involucrados en la interconexión de redes y servicios de Internet y correo electrónico, debe ser profesional, confidencial, ético y honesto, con el objeto de evitar situaciones que comprometan la imagen institucional.

1.5 Transmisión de Correos Electrónicos.

1.5.1 El manejo del correo electrónico implica su uso responsable para fines institucionales, en vista que es una herramienta de comunicación de la Entidad y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con esta normativa.

1.5.2 Para el uso del correo electrónico se debe de seguir los lineamientos siguientes:

- Es responsabilidad del usuario mantener la confidencialidad de la clave de acceso a su cuenta de correo, proporcionada por la Gerencia de Tecnologías de la Información.
- Cuando el usuario no utilice la computadora asignada, deberá cerrar o bloquear sesión, para evitar que otra persona tenga acceso a su cuenta de correo. La Gerencia de Tecnologías de la Información no se hará responsable si por descuido del usuario alguien manipula su cuenta de correo y/o borra algún correo.
- Sólo se debe abrir correos cuya fuente u origen sean de confianza del usuario.
- Antes de abrir los correos electrónicos con archivos adjuntos, debe explorarlos con el programa antivirus instalado por a la Unidad de Infraestructura y Seguridad Informática.
- El correo electrónico no debe ser utilizado para intercambiar chistes, música, presentaciones, pornografía o material que no sea del quehacer institucional, ni para enviar cadenas de carácter religioso o de otra índole.
- Antes de enviar información desde un país a otro, se debe asegurar no violar leyes del país en que opere.
- Los usuarios de las cuentas de correo electrónico institucional deberán revisar frecuentemente sus mensajes, asimismo depurarlos para mantener espacio disponible en su cuenta.
- El contenido y documentación o información remitida por el correo electrónico institucional es de responsabilidad del usuario que originó dicho envió.
- Evitar la remisión mensajes a listas globales. Las notificaciones institucionales no deberán ser un intercambio de correos. Son notificaciones.
- No remita cadenas de correo o cualquier otro esquema de pirámide de mensajes que genere SPAM.
- Los correos de carácter institucional y especialmente aquellos que serán enviados a un destinatario fuera de la institución, deberán contener la siguiente leyenda de PRIVACIDAD: “Este mensaje contiene información confidencial propiedad de la CONAMYPE y el destinatario; y no está permitida su copia, distribución o uso a personas no autorizadas. Si usted recibió este correo por error, por favor destrúyalo y notifique al remitente”.

- En vista que el uso de la cuenta de correo electrónico es exclusivo para desarrollo de actividades institucionales está prohibido su uso para fines personales, es decir, registro en aplicaciones o sitios web no vinculados a las labores, o comunicación de carácter personal.

- El jefe inmediato podrá tener acceso a las cuentas de correo de sus subalternos en caso de ausencia grave del empleado, esta solicitud se deberá de realizar a la Unidad de Infraestructura y Seguridad Informática quien dará un acceso temporal al jefe solicitante.

- La eliminación de mensajes de correo electrónico de carácter institucional se considerará una infracción grave, en tanto que es información institucional de acuerdo a lo establecido en la legislación vigente, por lo que deberá salvaguardarse. Se entiende que el correo electrónico no deseado o SPAM, no entra en esta categoría.

1.6 Recepción o Descarga de Software.

1.6.1. Previo a descargar software de Internet (incluido el software de licenciamiento libre), se debe obtener autorización del Jefe Inmediato o superior jerárquico en conjunto con la Jefatura de la Unidad de Infraestructura y Seguridad Informática, para llevar el control de los licenciamientos gratuitos.

1.6.2. No descargar software, si con esta acción viola las leyes de derechos de autor, propiedad intelectual, patente u otra relativa.

1.6.3. La instalación de cualquier tipo de software será realizada única y exclusivamente por personal de la Gerencia de Tecnologías de la Información.

1.6.4. El software descargado de Internet debe utilizarse bajo los términos autorizados por los derechos de autor, propiedad intelectual, patente, licencia interna y condiciones dispuestas por el Responsable que le autorizó.

1.6.5. No se debe permitir que personas fuera de la institución utilicen el software que se descargue de Internet o reproducirlo para uso personal o distribución.

1.7 Material Protegido por Leyes en la Web y Comunicación Digital

1.7.1 Se debe obtener autorización del jefe inmediato o autoridad superior previo a utilizar las marcas propiedad de la CONAMYPE (como Logotipos, frases publicitarias, etc.).

1.7.2 El autorizado a permitir que otras instituciones o personas utilicen las marcas de negocio propiedad de la CONAMYPE, debe asegurarse que se hayan firmado los documentos de consentimiento legal.

1.7.3 Se debe obtener autorización con validez legal, antes de publicar en Internet cualquier material protegido por las leyes de derechos de autor, propiedad intelectual o patente.

1.8 Uso de Internet como Medio de Investigación.

1.8.1 La información provista por Internet debe ser actualizada, exacta y precisa, razón por la cual se debe verificar su confiabilidad antes de tomar decisiones que pueden afectar negativamente a la institución, debiendo:

- Verificar la legitimidad del sitio visitado al momento de obtener información.

- No tomar o recomendar la toma de decisiones institucionales importantes, basadas en información obtenida en internet, sin antes verificar su integridad, ni obtener información de sitios de dudosa procedencia.

1.9 Prohibiciones al utilizar Internet.

1.9.1 Se prohíben desarrollar cualquiera de las siguientes actividades que pueden poner en riesgo la seguridad de la información del computador o la red de la Institución:

- Carga, descarga, distribución o acceso a pornografía.

- Colocar anuncios o enviar mensajes con información obtenida dentro de la institución, que perjudique la imagen de la CONAMYPE.

- Utilizar los servicios y recursos tecnológicos de la Institución con el fin de comercializarlos a otras partes o emplearlas para propósitos personales de negocio, dentro y fuera del horario de trabajo.

- Utilizar sus conocimientos y habilidades sobre las técnicas de conexión y acceso remoto a redes para llevar a cabo actividades de espionaje, interceptar, bajar, desviar o retransmitir información delicada y/o confidencial.

- Utilizar Internet o el Correo Electrónico cuando esta acción viole sus obligaciones como empleado; como pretender hablar en nombre de la institución, utilizar logotipos, frases publicitarias o material exclusivo de la CONAMYPE.

- Acceso a sitios de descargas (películas, música, programas, juegos, servicios de radio, fotos, TV y videos en línea).

- Hacer uso de dispositivos para conectarse a Internet sin tener la autorización correspondiente.

- Realizar actividades externas con fines de lucro.

- Utilizar programas P2P para realizar cualquier tipo de descarga.

- Acceder al servicio de internet y correo electrónico para ver, anunciar, transmitir, descargar o distribuir información de cualquier tipo, si esto da lugar a infracciones o violaciones en las Políticas, Reglamentos, Normas, Procedimientos institucionales o de algún contrato privado celebrado con clientes, funcionarios o empleados.

ANEXOS

Anexo 1. Solicitud de Cambio de Contenidos en Base de Datos de Producción.

Anexo 2. Solicitud de Autorización para Conexión a Internet y Correo Electrónico.

Anexo 3. Solicitud de Autorización para Conexión a Internet por Medio de Modem Inalámbrico.

Anexo 4. Formato de respaldo de información de equipo informático.

Anexo 1. Solicitud de Cambio de Contenidos en Base de Datos de Producción.

Fecha de solicitud: _____ Requerimiento (Requerimiento)#: _____

Unidad a la que pertenece la persona usuaria	
Nombre de la persona usuaria	

Seleccione en que módulo del sistema ocurrió el inconveniente						
SISTEMA INTEGRADO		SGI		PEI POA		
PLAN DE ACCIÓN PERSONAL		FINANZAS				
TALENTO HUMANO		PAPELERIA		OTROS, especifique:		
CONSULTORES		ACTIVO FIJO				
SISTEMA DE PLAZAS		REGISTRO MYPE				
VEHICULOSY COMBUSTIBLE		GESTION CONOCIMIENTO				
Especifique datos/reporte específico con inconveniente(s)						
Especifique el dato/reporte correcto que debe establecerse						

F:_____ Sello

Director(a)/Gerente(a)/Jefe(a)/Coordinador(a)

Responsable de la aplicación o cambio

Anexo 2. Solicitud de Autorización para Conexión a Internet y Correo Electrónico.

Fecha de Solicitud: _____

Lugar: ❑ Oficina Central ❑ Oficina Regional_____

Por este medio, solicito se realice la instalación y conexión de los siguientes servicios:

Creación y configuración de Correo Electrónico: ❑

Conexión y configuración de acceso Internet por medio de:

❑ Red Institucional ❑ Acceso Remoto

Con el siguiente nivel de acceso:

Nivel de Acceso	Marque una opción	Descripción
Acceso total	❑	Acceso libre a sitios de Internet y descargas
Acceso Parcial	❑	Acceso solo a navegación Web (no redes sociales)
Solo Correo	❑	Uso únicamente a correo electrónico

Los servicios arriba indicados se asignarán a:

_____

Unidad Organizativa:

_____

Al momento de firmar el presente documento, en cualquiera de las formas posibles, ***el empleado se da por enterado de las sanciones que puede recibir en caso de violar cualquiera de las normativas y procedimientos vigentes.***

Nombre del Empleado: _____ Firma: _____

Nombre de la Jefatura de la Unidad Organizativa: _____

Firma y Sello: _____

Nota: El Jefe de la Unidad Organizativa que solicita el uso de los servicios, es responsable de haber informado al usuario acerca de las “Normas de Uso de Internet y Correo Electrónico”, por lo tanto, el usuario *está* ***enterado de los derechos y obligaciones al respecto.***

Anexo 3. Solicitud de Autorización para Conexión a Internet por medio de modem inalámbrico.

Fecha de Solicitud: _____

Lugar: ❑ Oficina Central ❑ Oficina Regional

_____

Servicio solicitado: Conexión e Instalación de Internet móvil ❑

Justificación:

_____

_____

_____

Por este medio, solicito se realice la instalación y conexión del equipo en la computadora asignada a:

_____

_____

Unidad Organizativa:

_____

Al momento de firmar el presente documento, en cualquiera de las formas posibles, ***el empleado se da por enterado de las sanciones que puede recibir en caso de violar cualquiera de las normativas y procedimientos vigentes.***

Que el uso de un dispositivo móvil para conexión, no lo exonera de la aplicación de las normas para el uso de equipo, así como del uso de Internet.

Nombre del Empleado: _____

Firma: _____

Nombre del Jefe de la Unidad Organizativa: _____

Firma y Sello: _____

Nota: El Jefe de la Unidad Organizativa que solicita el uso de los servicios, es responsable de haber informado al usuario acerca de las “Normas de Uso de Internet y Correo Electrónico”, por lo tanto, el usuario *está* ***enterado de los derechos y obligaciones al respecto.***

Anexo 4. Formato de respaldo de información de equipo informático

Fecha: _____.

Este día a las _____ horas se realizó la copia de seguridad de los documentos y archivos que contiene el

Ordenador de tipo _____ con código de activo fijo (SAF) _____ asignado a

_____

Qué entrega el puesto de _____

La copia de seguridad fue realizada por

_____

Unidad de Infraestructura y Seguridad Informática

Gerencia de Tecnologías de la Información

Comisión Nacional de la Micro y Pequeña Empresa

DISPOSICIONES FINALES

1) Cualquier situación no prevista en el contenido del presente documento, será resuelta por la Junta Directiva o la Presidencia, en base a los respectivos dictámenes técnicos legales y las facultades que les correspondan.

2) Para efectos de determinación de responsabilidades y sanciones, se atenderán los procesos establecidos en la normativa legal que corresponda y lo que determine la Ley de la Corte de Cuentas de la Republica.

VIGENCIA

La presente Normativa entrará en vigencia a partir de la fecha de su divulgación al personal.