Plan de Contingencia Para la Unidad de Sistemas y Tecnología de Información del Gobierno Autónomo Descentralizado Antonio Ante en Base a la Norma Iso/Iec 27002.

Luis D. Narváez, Karina A. Méndez
ldnarvaez@utn.edu.ec., kary_3040@yahoo.es

Resumen ― *El presente trabajo analiza una metodología para el desarrollo de un Plan de Contingencia para los Sistemas de Información, se definen acciones generales para asegurar la adecuada recuperación de información y de los servicios informáticos dentro de la organización; esta metodología comprende el análisis e identificación de riesgos, identificación y evaluación de amenazas y vulnerabilidades, estimaciones de impacto, la probabilidad de ocurrencia, evaluación de escenarios de contingencia, las protecciones necesarias, así como también la definición soluciones y estrategias que permitan garantizar la continuidad de las actividades en caso de materializarse dichas amenazas.*

Tener presente que no existe un sistema 100% seguro, ya que los riesgos siempre están presentes, a pesar de las medidas que se tomen para prevenirlo.

***Términos para la indexación*― La Seguridad de la información, Plan de Contingencia.**

I. Introducción

Un Plan de Contingencia Informático es un conjunto de actividades que nos permiten realizar acciones para minimizar los riesgos en caso de algún desastre de origen natural o humano, manteniendo la operatividad de las actividades a un mínimo nivel hasta recuperar la totalidad de los sistemas y recursos; un plan de contingencia se encuentra conformado por tres acciones fundamentales que son: prevención, detección y recuperación.

Prevención: son acciones que nos ayudan a prevenir cualquier eventualidad que afecte las actividades de las organizaciones de manera total o parcial a fin de reducir los impactos producidos.

Detección: Son las acciones que se deben tomar durante o inmediatamente después de la materialización de la amenaza a fin de disminuirla.

Recuperación: Se definen los procesos o lineamientos que se deben seguir después de haber controlado la amenaza, en este plan se realiza la restauración de los equipos y actividades a su estado inicial antes de materializarse la amenaza.

II. Términos y Definiciones Básicas

A. Información — La información la podemos encontrar de diferentes formas, en papel o de manera digital, la información siempre debe contar con medidas de seguridad a fin de evitar pérdidas o modificación de datos que puedan poner en riesgo la continuidad de las actividades de la organización.

B. Seguridad de la información ― conjunto de reglas, controles y procedimientos que adoptan las organizaciones para salvaguardar la información de las diferentes amenazas como fraudes, espionajes, vandalismos, incendios, inundaciones, software maliciosos, ataques de terceros, negación de servicios, etc.

C. Amenaza ― revelación no autorizada de la información sin modificar el estado del sistema.

D. Riesgo― una vulnerabilidad explotada por una o varias amenazas que al materializarse provocan daños e interrupciones de los servicios y procesos de información.

E. Vulnerabilidad ― Es una debilidad en la seguridad de la información que puede dar lugar por diferentes causas como por ejemplo la falta de mantenimiento, falta de conocimiento en el

personal, desactualizaciones de los sistemas críticos, etc.

III. BASES DE LA SEGURIDAD DE LA INFORMACIÓN

"No existe un sistema 100% seguro, ya que los riesgos siempre están presentes, a pesar de las medidas que se tomen para prevenirlo."

Con esta frase podemos decir que no existe un sistema totalmente seguro, pero si un sistema confiable, el mismo que se basa en 3 pilares fundamentales de la seguridad de información como se observa en la fig.1.

Fig. 1. Seguridad de la información según la norma ISO/IEC 17799

Confidencialidad: Característica que garantiza que la información sea accesible sólo para las personas autorizadas a tener acceso a la misma.

Integridad: Característica que conserva la exactitud y totalidad de la información, asegurando que la información llegue completa y sin modificaciones.

Disponibilidad: Garantiza que los usuarios autorizados tengan acceso a la información siempre que la requieran.

IV. SISTEMAS DE INFORMACIÓN

Un sistema de información se encuentra conformado por tres elementos como son: la información, recursos humanos y equipos computacionales que operan en conjunto para realizar actividades de administración, almacenamiento, procesamiento, transmisión o recepción datos e información con el único propósito de cumplir con los objetivos de la organización.

Entrada: captura de datos tanto desde el interior como del exterior del sistema de información.

Procesamiento: convertir datos e información de una manera más significativa para el negocio.

Salida: transferir la información ya procesada a los usuarios para que desarrollen sus actividades diarias.

En la fig.2 se observa de manera gráfica el proceso que se realiza en un sistema de información

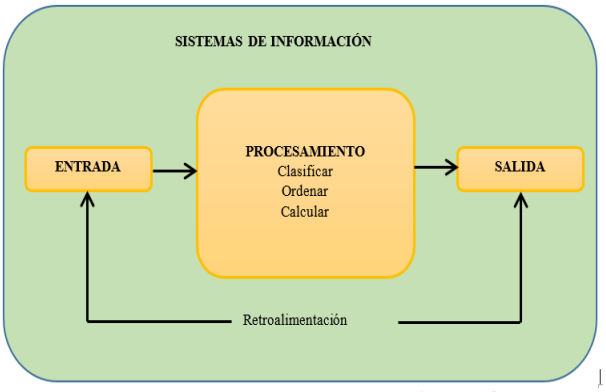

Fig. 2. Proceso de un Sistema de Información

V. CARACTERÍSTICAS DEL PLAN DE CONTINGENCIA INFORMÁTICO.

Un plan de contingencia eficaz, minimiza los daños ocasionados a la organización producto de la materialización de las amenazas de origen natural o por errores humanos, por consiguiente debe cumplir con las siguientes características:

- *Aprobación*: Debe ser aprobado por la dirección y los usuarios.
- *Flexibilidad*: Debe poder adaptarse a cualquier contingencia, no debe ser específico para un solo desastre.
- *Mantenimiento*: Ser preciso, evitar detalles innecesarios para que pueda ser actualizado.
- *Costo-efectividad*: Las medidas aplicadas en cada una de las eventualidades deberán ser evaluadas con relación a las ventajas que nos brindan, deben ser razonables.
- *Respuesta organizada:* Contar con una lista de las acciones y servicios que deben recibir prioridad.
- *Responsabilidad:* Contendrá el nombre de los responsables que deben asumir las diferentes funciones en caso de una emergencia.
- *Pruebas:* Se realizarán pruebas con inventarios de tiempo y procedimientos de respaldo, debe tener una metodología.

VI. FASES DE UN PLAN DE CONTINGENCIA INFORMÁTICO

A. *Planificación*— contempla actividades como el diagnóstico inicial de la situación actual de la institución, diseño de propuestas para un determinado problema,

diagnóstico de la estructura organizacional, servicios que brindan a la ciudadanía, servicios consumidos, materiales utilizados y el inventario de los recursos informáticos, haciendo uso de herramientas automatizadas o de forma manual mediante la recopilación de información, así como también la delimitación del alcance del plan de contingencia.

B. Identificación de escenarios de contingencia y amenaza — se obtiene de la información adquirida de los riesgos críticos, identificarlos, conocer las causas y el impacto que generarían para la organización si llegan a materializarse. En el diagrama 1 se observa los posibles escenarios de contingencia que ponen en riesgo la seguridad de la información.

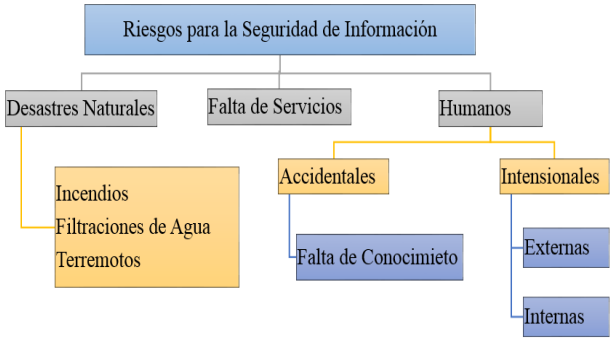

Diagrama 1. Riesgos para la Seguridad de la información

Desastres naturales: terremotos, incendios, inundaciones o filtraciones de agua.

Desastres por falta de servicios: fallas en el sistema de energía, ventilación y en el sistema de seguridad, en la red de datos, los equipos de networking y servidores.

Fallas por terceros: errores humanos, denegación de servicios, software malicioso virus informáticos, vandalismos, espionajes, suspensión en el procesamiento de información.

C. Evaluación de Riesgos — para la evaluación de los riesgos se debe identificar, cuantificar y priorizar los riesgos dentro de la organización, los resultados obtenidos deben proporcionar la información necesaria para realizar una adecuada gestión de riesgo mediante la implementación de controles de protección contra los riesgos identificados; se considera el siguiente proceso:

1. Identificación de los riesgos.
2. Evaluar de los riesgos en términos de impacto y probabilidad de ocurrencia.
3. Establecer un orden adecuado de prioridad en el tratamiento de los riesgos.
4. Identificar el tiempo máximo de interrupción permitida en los servicios y procesos críticos.
5. Definir la designación de roles de trabajo y obligaciones al personal en caso de emergencia.
6. Realizar un monitoreo continuo de los riesgos.

D. Identificación de Vulnerabilidades Tecnológicas
Se hace uso de la lista de los activos y los controles existentes dentro de la organización, las vulnerabilidades se pueden encontrar en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software o equipos de comunicaciones.

Para la evaluación de las vulnerabilidades tecnológicas se hace uso de diferentes técnicas o métodos por ejemplo la utilización de herramientas de software de exploración automática, entrevistas, cuestionarios, inspecciones físicas entre otros; todo dependerá de la importancia del sistema de tecnología de información y los recursos disponibles.

Los criterios para la evaluación de las vulnerabilidades tecnológicas de establecen de la siguiente manera:

TABLA I
CRITERIOS DE EVALUACIÓN DE VULNERABILIDADES TECNOLÓGICAS

Características Denominación	Facilidad de Explotación	Capacidad de Detección	Costo de Recuperación
Alta	Probable	Difícil	Alto
Media	Probable	Posible	Alto
Baja	Probable	Posible	Mínimo
Mínima	Poco Probable	Probable	Mínimo

E. Valoración de los activos — Una vez identificado los activos de mayor relevancia dentro de la organización se procede a la definición de una escala de valoración para cada uno de los activos críticos identificados dentro de la organización; la valoración puede ser de forma cuantitativa como cualitativa

En la tabla 2 se observa las diferentes características para la asignación de un valor a cada uno de los activos de la organización.

TABLA II
VALORACIÓN DE LOS ACTIVOS

VALORACIÓN DE LOS ACTIVOS				
Valor	**Denominación**	**Disponibilidad**	**Integridad**	**Confidencialidad**
4	Critico	La información, instalaciones y recursos siempre debe estar disponibles Su pérdida es considerada como catastrófica para la Institución.	Toda información, instalación o recurso donde la integridad es importante y debe garantizarse Su pérdida seria catastrófica.	Abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
3	Alto	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
2	Medio	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Todo recurso, información o instalación en el cual la integridad es de importancia media y debe garantizarse.	Información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
1	Bajo	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.

Los criterios que se considera para la asignación de los valores:

- El costo original del activo.
- El valor original por pérdida de confidencialidad, disponibilidad e integridad.
- El impacto generado para la organización por los años o suspensión de los servicios.

F. Análisis de riesgo – dentro de una organización el análisis de los riesgos nos permite identificar activos, controles de seguridad, criterios de diseño y evaluación de planes de contingencia. El análisis de riesgos se encuentra comprendida por tres elementos que permiten dar un valor los riesgos dentro de la organización: probabilidad de ocurrencia del riesgo, el impacto del riesgo y la determinación del riesgo.

1. *Probabilidad de ocurrencia* de una amenaza – se establece bajo qué circunstancias el activo tendrá valor o necesitara protección, se determinara en base a estadísticas recogidas a lo largo de la administración y se considerara lo siguiente:

- La importancia del activo para la organización.
- La facilidad de explotación de una vulnerabilidad en el activo.
- La susceptibilidad técnica de la vulnerabilidad a la explotación.

1.1. *Evaluación de probabilidad de riesgo* – se realiza mediante la identificación de las amenazas, los activos afectados y las vulnerabilidades, también se tomara en cuenta la frecuencia con la que las amenazas ocurren.

En la tabla 3 se define las cuantificaciones para la designación de la frecuencia de cada una de las vulnerabilidades encontradas.

TABLA III
PROBABILIDAD DE OCURRENCIA

Nivel	Denominación	Descripción
76-100 %	Muy Frecuente	Eventos repetitivos
51-75%	Frecuente	Eventos aislados
26 -50 %	Ocasional	Sucede alguna vez
0 -25%	Remoto	Imposible que suceda

2. *Impacto del Riesgo* – se define como una eventualidad dentro de la seguridad de la información que puede afectar a más de un activo dentro de la organización, estos impactos pueden ser inmediatos o futuros que provocarían pérdidas financieras. El impacto inmediato puede ser directo cuando se necesita el remplazo del activo perdido, configuración, instalación o copia de soporte, el costo de las operaciones suspendidas debido al incidente; o indirecto cuando la afectación es la pérdida de oportunidades por los daños producidos en este equipo, cuando se utilizaron recursos que pudieron usarse en otra parte y los costos por interrupción de las actividades.

Los criterios para la determinación del impacto en los activos son las siguientes:

- El grado de afectación o el costo que implicaría para la organización si se produce algún daño o la interrupción de un proceso crítico.

- De acuerdo a la importancia de los activos de la institución.
- Las brechas de seguridad que existen tanto a nivel de lógico como físico.
- Las operaciones que se realizan tanto al interior como al exterior.
    - El valor financiero para la organización si sufre alguna emergencia.

En la tabla 4 se define los valores para determinar las prioridades de evaluación del impacto.

TABLA IV
PRIORIDADES DE EVALUACIÓN DEL IMPACTO

Impacto	Valor	Descripción
Bajo	1	Cuando no afectan las actividades y los sistemas principales trabajan de forma normal.
Medio	2	Cuando los daños son parciales y se dan en los sistemas, no afecta a las operaciones.
Alto	3	Cuando se ven afectadas de manera directa las operaciones y funciones, los usuarios y los sistemas informáticos.
Critico	4	Pérdida de información crítica, daños severos en los equipos, Suspensión de funciones

3. *Determinación del Riesgo* – se establece mediante el la determinación del impacto de las amenazas sobre los activos críticos por la probabilidad de ocurrencia de cada una de las amenazas. En la figura 3 se observa de manera gráfica la determinación de los niveles de riesgo.

PROBABILIDAD				
4	**A**	**A**	**C**	**C**
3	**M**	**M**	**A**	**C**
2	**B**	**M**	**M**	**A**
1	**B**	**B**	**M**	**A**
	1	2	3	4

IMPACTO
Fig. 3. Niveles de Riesgo

- El rojo nos indica los riesgos críticos (C)
- El naranja no indica que son riesgos altos (A)
- El amarillo son riesgos medios (M)
- El verde no indica los riesgos bajos (B)

G. Tipos de análisis de Riesgos - La estimación del riesgo se define de acuerdo a diferentes niveles de detalle dependiendo de la criticidad de los activos y vulnerabilidades conocidas. La estimación de riesgos se puede realizar de dos formas: cuantitativo y cualitativo.

*Cualitativo***:** Cuando usamos adjetivos calificativos como alta, media baja, mediante estos podemos describir las consecuencias o probabilidades de ocurrencia de un riesgo

*Cuantitativo***:** La estimación cuantitativa permite dar valores numéricos tanto para las consecuencias como para la probabilidad de ocurrencia, utiliza como fuente datos de incidentes anteriores.

H. Identificación de controles preventivos – permiten brindar alternativas eficientes que minimicen la aparición de vulnerabilidades, estos procedimientos deben ser documentados junto con las causas que lo provocaron y las acciones tomadas.

Se considera lo siguiente:

- La formación de equipos que brinden soporte en caso de una contingencia.
- La asociación de soluciones con cada riesgo identificado.
- Determinar procesos críticos y el impacto para la organización si estos fallan.
- Identificar una perdida aceptable de información y servicios
- Mantener actualizado el documento donde se encuentras las soluciones y reglas de implementación.

I. Estrategias de Protección Tecnológica - Se debe definir una estrategia de recuperación que contenga una guía de procedimientos para la recuperación ante el desastre, la elección de la misma se determinará de acuerdo a la criticidad de los procesos o aplicaciones, tiempo de recuperación y la seguridad requerida. De acuerdo al tipo de organización existen diferentes tipos de centros de recuperación, a continuación se detalla algunos tipos de centros hardware de respaldo en sede remota.

En la tabla 5 se determina el tipo de centros de recuperación de información de acuerdo a las necesidades de cada institución.

TABLA V
PROBABILIDAD DE OCURRENCIA

Centros de Recuperación	Compatibilidad	Costo de Instalación
Hot sites:	Total en software y hardware uso inmediato	Medio alto
Warm sites:	Configuración parcial del centro primario, hay q esperar para su uso	moderado
Cold sites:	infraestructura básica, electricidad, salas para instalar equipos	Bajo
Centro duplicado:	Redundancia de equipos solo de los procesos críticos diseñados para entrar en funcionamiento al instante de haber declarado una emergencia.	Elevado

VII. DOCUMENTACIÓN DEL PROCESO

Después de haber realizado el análisis de los riesgos y elaborar una serie de recomendaciones en caso de alguna eventualidad o desastres se procede a la documentación de lo descrito anteriormente en las etapas. Este documento debe ser redactado en un lenguaje simple y entendible para todos.

Debe contener la siguiente información:

- Conocer la situación previa al desastre.
- Contar con información de los riesgos.
- Identificar procesos y recursos de Infraestructura de telecomunicaciones que se debe recuperar.
- Designación de responsabilidades y soluciones a realizar en caso de contingencias.

Se debe realizar una revisión continua del plan de contingencia establecido, pues tanto la tecnología como el negocio crecen, evolucionan y lo que en este momento es útil más adelante será obsoleto.

Para un adecuado mantenimiento del plan de contingencia es importante considerar lo siguiente:

- Las necesidades del negocio.
- La adquisición de nuevo hardware o desarrollo de nuevas aplicaciones de software.
- Los procesos críticos cambian de acuerdo a las necesidades del negocio.

VIII. REALIZACIÓN DE PRUEBAS Y VALIDACIÓN DE LOS PLANES DE CONTINGENCIA

Las pruebas en un plan de contingencia nos permite asegurar que tanto el equipo de recuperación como el resto del personal deben conocer sus responsabilidades para el restablecimiento de la operatividad de la red y la seguridad de la información; las pruebas deben contemplar la siguiente información.

a) Verificar que la información del plan este correcta y completa.
b) Evaluación del personal involucrado.
c) Evaluación de la coordinación entre el equipo de emergencia y componentes externas.
d) Evaluación de la capacidad de recuperación.
e) Evaluación del rendimiento general de la organización después de la recuperación.

IX. NORMAS Y ESTÁNDARES DE SEGURIDAD

ISO/IEC 27000 es un conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

A. ISO 27000: Contiene términos y definiciones que se emplean en toda la serie 27000. Es gratuito, a diferencia de las demás de la serie, que tienen un costo.

B. ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del SGSI. Permite establecer condiciones de transición para aquellas empresas certificadas.

C. ISO 27002: Publicada el 1 de Julio de 2007. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.

D. ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

E. ISO 27011: Publicada a finales de 2008. Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU.

F. ISO 27031: Publicada en Mayo de 2010. Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

G. ISO 27032: Publicada en Febrero de 2009. Consiste en una guía relativa a la ciberseguridad.

X. CONCLUSIONES

El desarrollo del diseño de un plan de contingencia informático permite conocer las vulnerabilidades latentes en infraestructura de red y servicios dentro de la institución, y pone a consideración de las autoridades los respectivos correctivos a fin de minimizar los riesgos.

La identificación, evaluación de los riesgos y escenarios de contingencia en los activos considerados críticos para la institución se realizó en base a perfiles de amenazas, considerando el impacto ocasionado si llegan a materializarse dichos riesgos.

Se definen recomendaciones para el control y administración de la red de la institución que permitan asegurar la operatividad de la red al mínimo de su

capacidad con la finalidad de minimizar pérdidas económicas y de reputación.

La formación de grupos de emergencia en el departamento informático permitirá mayor organización al momento de dar una respuesta ante una incorrupción de servicios.

Con las estrategias propuestas para el mejoramiento de la seguridad de la información y la reducción de amenazas en los activos críticos se mejorará la eficiencia y administración de la red y los servicios proporcionados por el departamento de sistemas del GAD de Antonio Ante.

Finalmente se concluye que, una institución provista de un plan de contingencia informático va a estar preparada para eventos inesperados, tomar medidas oportunas y soluciones eficientes.

XI. REFERENCIAS

[1] Acuerdo No. 166. (09 De 2013). *Esquema Gubernamental De Seguridad De La Información (Egsi). Quito, Ecuador.*

[2] Areitio, J. (2008). *Seguridad De La Información (Redes Informáticas Y Sistemas De Información). Madrid: Learminig Paraninfo Sa.*

[3] Contraloría General De La República. (2009). *Normas Tecnicas En Tecnologías De Información Y Comunicaciones. Obtenido De Http://Www.Hacienda.Go.Cr/Cifh/Sidovih/Spaw2/Uploads/Images/File/Normas%20t%C3%A9c%20en%20ti%20y%20comunics.Pdf*

[4] Hernández, I. J. (Diciembre De 2005). *Métodos Y Políticas De Respaldo En Planes De Contingencia. Obtenido De Http://Benjamin.Davy.Free.Fr/Auditoria/Contingenciaybackupensi.Pdf*

[5] Herrero, R. (2010). Planes De Contingencia Y Su Auditoría.

[6] Instituto Del Mar De Perú. (2012). *Plan De Contingencia Informático.*

[7] Katz, M. (2013). *Redes Y Seguridad. Alfaomega.*

[8] Nacional Institute Of Standars And Technology. *(Mayo De 2010). Contingency Planning Guide For Federal Information Systems.*

[9] Ntc-Iso 27005. (S.F.). *Http://Es.Scribd.Com/Doc/124454177/Iso-27005-Espanol. Obtenido De Http://Es.Scribd.Com/Doc/124454177/Iso-27005-Espanol*

[10] Nte Inen-Iso/Iec 27002. (2009). *Tecnología De La Información-Técnicas De La Seguridad-Código De Prácticas Para La Gestión De La Seguridad De La Información. Quito, Ecuador.*

XII. BIOGRAFÍAS

Narváez David. Nació en Ibarra-Ecuador el 26 de Octubre de 1985. Obtuvo el título de Bachiller en Ciencias en el 2003. Luego obtuvo el grado de Ingeniero en Electrónica y Redes de Comunicación en el 2012. Actualmente Egresado de la Maestría en Tecnologías. Se desempeña desde hace 3 años como Docente de la Faculta de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.
Email: ldnarvaez@utn.edu.ec.

Méndez Karina. Nació en Ibarra-Ecuador el 20 de octubre de 1989. Obtuvo el título de Bachiller Técnico con especialización en Informática en el 2007, Colegio Nacional "Ibarra". Actualmente Egresada de la carrea de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte**.**