PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

Denominación del Programa de Formación: **APLICACIÓN DE HERRAMIENTAS DE INFORMACIÓN Y COMUNICACIÓN**

- Código del Programa de Formación: **13120373**
- Nombre del Proyecto: N/A
- Fase del Proyecto: N/A
- Actividad de Proyecto: N/A
- Competencia:
- APLICAR TECNOLOGÍAS DE LA INFORMACIÓN TENIENDO EN CUENTA LAS NECESIDADES DE LA UNIDAD ADMINISTRATIVA.

- Resultados de Aprendizaje Alcanzar:

APLICAR HERRAMIENTAS WEB Y DE TRABAJO COLABORATIVO DE ACUERDO CON LA INFORMACIÓN

UTILIZAR LAS HERRAMIENTAS OFIMÁTICAS DE ACUERDO CON LA INFORMACIÓN A PROCESAR

UTILIZAR LA HERRAMIENTA DE ADMINISTRACIÓN DE ARCHIVOS DE ACUERDO CON EL SISTEMA OPERATIVO

OPERAR EQUIPOS AUDIOVISUALES Y DE CÓMPUTO DE ACUERDO CON PROCEDIMIENTOS ESTABLECIDOS

- Duración de la Guía: **40 Horas**

2. PRESENTACIÓN

Las Tecnologías de la Información y Comunicación (TIC) como herramienta de teletrabajo, ha tomado un papel fundamental hoy en día, más aun debido a la Pandemia Mundial ocasionada por el virus del COVID-19. La necesidad de poder continuar con los procesos laborales con los usuarios y cuerpo administrativo, que les permitan seguir brindando la posibilidad de continuar el intercambio de ideas, experiencias y conocimiento desde sus hogares mediante el uso de herramientas que faciliten la comunicación, creación, almacenamiento y reutilización de contenidos, han originado que el modo presencial tradicional de prestación de servicios al que muchos funcionarios estábamos acostumbrados esté cambiando debido a las demandas sociales, necesidad de evolución y adaptación a los nuevos modelos tecnológicos y de comunicación. Por esto, se hace necesario en los funcionarios y personal administrativo, despertar interés por emplear de manera eficiente herramientas que permiten promover y estimular los talentos potenciales

del individuo y continuar sus procesos laborales desde sus hogares. Logrando así un tipo de educación personalizada, colaborativa, participativa y que se centre en alcanzar diferentes objetivos y competencias.

Por lo anterior, el Centro de Comercio y Servicios del SENA Regional Cauca se ha dado a la tarea de impartir el curso de Ciudadanía Digital para la Paz, con el propósito de crear competencias tecnológicas que les permitan brindar atención al personal interno y externo de la organización, en la situación actual por la que atraviesa el País debido al COVID-19.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

Apreciado Funcionario, el aprendizaje autónomo y el trabajo colaborativo son las fuentes del conocimiento, aquí radica la importancia del trabajo en equipo con el fin de fortalecer las habilidades y destrezas que manejadas con responsabilidad forjaran el perfil profesional, personalidad y carácter critico para la toma de decisiones de cada uno de los miembros de una empresa.

En esta guía usted desarrollara los conocimientos, habilidades y destrezas necesarias para el conocimiento y manejo adecuado mediado por herramientas tecnológicas TIC de Apoyo a sus funciones laborales, para continuar prestando servicios a la ciudadanía en general desde sus hogares, permitiendo con esto desarrollar un proceso personalizado, colaborativo, participativo.

Uso de las herramientas tecnológicas

El uso de tecnologías como apoyo laboral tiene un impacto positivo en la prestación de servicios organizacionales, dadas sus características de disponibilidad, de variedad de información en tiempo real, facilidad de acceso y divulgación de la información sin desplazarse a una entidad u oficina de manera personal, que le dan dinamismo al proceso en sí.

Para promover ese potencial disponible, se hace pertinente el diseño de estrategias basadas y aplicadas con las herramientas de comunicación y comunicación existentes, proceso de capacitación en el que se motive a los funcionares de cualquier entidad a conocer y aprender a utilizar cada una de las herramientas TIC y las incorpore a sus actividades diarias. Se debe tener claro que estas herramientas son sólo un apoyo para la prestación de sus servicios o realización de labores diariamente realizadas en una empresa y el aplicarlas de manera consciente se puede reflejar en mayor calidad en la prestación de servicios de la organización.

Es importante señalar el grado de responsabilidad de los funcionarios y personal administrativo en el aprovechamiento y uso adecuado de estas herramientas tecnológicas, que impacte de forma positiva en la mejora de las habilidades y competencias que se requieran para la prestación de sus servicios a la comunidad.

Actividad 5.

El Aprendiz deberá responder un cuestionario referente a la Unidad 5 del curso de Ciudadanía Digital para la Paz, ingresando al link suministrado por el instructor.

Para esta actividad, será el Instructor quien revisara los resultados del cuestionario.

UNIDAD 4 SEGURIDAD DE LA INFORMACIÓN

OBJETIVO:

La gestión de la seguridad es el componente clave y primario para un plan exitoso de protección de la información en una PyME. Sin gestión no hay controles o medidas que provoquen un aseguramiento eficiente de los datos de la organización, o se evalúen los riesgos a los cuales se está expuesto.

1. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

Los objetivos mencionados brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.

Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos

2. POLÍTICAS DE SEGURIDAD

Una Política de Seguridad es "*una* declaración de intenciones *de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán*".

3. POLITICA DE BACKUPS

Se denomina backup (o copia de seguridad) a la copia de información y su almacenamiento fuera de entornos de producción.

4. POLÍTICAS DE MANEJO DE INCIDENTES

La prevención ante incidentes es un componente clave de la seguridad en la empresa. Sin embargo, la probabilidad de ocurrencia de un incidente de seguridad existe, independientemente de las medidas de seguridad aplicadas.

5. INFORMACIÓN

De acuerdo con la Norma Técnica Colombiana NTC-ISO/IEC 27002 (2007):

“La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno de negocios cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

6. CLASIFICACIÓN DE LA INFORMACIÓN

En un programa de seguridad es necesario identificar la criticidad de la información. Esto permite a la empresa determinar cuántos recursos (tanto económicos, humanos, como de otra índole) serán asignados a la protección de dicha información

7. CARACTERISTICAS PRINCIPALES DE LA INFORMACIÓN.

Cuando ocurre un ataque cibernético, el objetivo principal del atacante es robar y/o afectar la información y sus características, por lo que es recomendable tomar medidas

8. SISTEMAS DE INFORMACIÓN

Se considera un sistema de información al conjunto de elementos interrelacionados entre sí, a través de los cuales se recoge, procesa, analiza y distribuye la información, que sirve para apoyar la toma de decisiones en una empresa u organización.

9. COMPONENTES DE UN SISTEMA DE INFORMACIÓN

De forma general se puede decir que los componentes de un sistema de información son: Recursos humanos, datos, hardware, software y procedimientos administrativos.

10. ACTIVIDADES DE UN SISTEMA DE INFORMACIÓN

A través de un sistema de información se realizan cuatro actividades básicas como: entrada, almacenamiento, procesamiento y salida de información.

11. ACTIVOS DE INFORMACIÓN

Son los componentes necesarios e indispensables para el funcionamiento de un sistema informático.

12. VALORACIÓN DE ACTIVOS

Significa evaluar la importancia que tienen para la operación y el sustento de la organización.

13. RIESGOS INFORMÁTICOS Y ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO

Las amenazas en un sistema de información, pueden provenir de diferentes fuentes: externas e inclusive internas. Un hacker remoto que entra al sistema a través de un troyano: programas de descarga gratuita que ayuda a gestionar fotos pero es una puerta trasera a nuestro sistema permitiendo la entrada de espías. El personal de nuestra organización, que conoce nuestras vulnerabilidades. Estas amenazas pueden ser Lógicas, Físicas, y Personas.

14. SEGURIDAD EN REDES

Las personas y organizaciones dependen en la actualidad de sus computadoras. Las herramientas de correo electrónico, administración de archivos, contabilidad y gestión de la información, resultan de vital importancia en una empresa. Debido a esto, las intrusiones de personas no autorizadas en la red (interna o externa) causan interrupciones costosas y pérdidas de trabajo.

15. RIESGOS EN INTERNET.

En internet se encuentra información de muchos temas, por lo que al hacer uso de este o realizar alguna consulta, daremos tener en cuenta los riesgos mas comunes al navegar en la red

16. CONSEJOS PARA UNA NAVEGACIÓN SEGURA

Guía practica de consejos a tener en cuenta en el momento de realizar una navegación en internet.

17. CONSEJOS DE SEGURIDAD GENERALES

Pautas de seguridad que toda empresa y persona debe tener en cuenta para estar seguro y proteger sus datos.

18. CONSEJOS PARA NAVEGAR SEGURO

Lista de sugerencias que permiten que el usuario haga un uso más seguro tanto del navegador, como de los sitios y servicios que son accedidos a través de este.

19. CONSEJOS EN GENERACIÓN DE CLAVES O CONTRASEÑAS

Consejos de buenas practicas y generación de contraseñas seguras.

20. CONFIGURARCIONDE SEGURIDAD DE SISTEMA OPERATIVO

Practicas a realizar para configurar correctamente nuestros equipos informáticos de ataques maliciosos.

21. CONSEJOS DE USO DE CORREO ELECTRÓNICO

Consejos para un adecuad uso de nuestros correos electrónicos que permitirán salvaguardar nuestros datos de posibles hurtos de información.

22. CONSEJOS DE USO DE BANCAS VIRTUALES Home Banking

Al acceder a Internet se puede ser víctima de innumerables amenazas y engaños. Esto toma énfasis al tratarse de la manejo de información sensible como la banca en línea (o *e-banking)*.

23. SEGURIDAD EN REDES SOCIALES

Actualmente las redes sociales son muy populares y los usuarios las utilizan masivamente; estas características las transforman en importantes focos de propagación de malware. Por tal motivo se torna necesario tener en cuenta y aplicar medidas preventivas

24. CIFRADO DE INFORMACIÓN

El objetivo de cifrar (o encriptar) la información puede ser, de acuerdo a como se aplique, mantener la confidencialidad, integridad, autenticidad y no repudio de la información; de esta manera se cubre el espectro más amplio en lo que a seguridad de la información concierne. Actualmente también es utilizado por cierto tipo de malware (ver ransomware en capítulos anteriores).

25. CONSECUENCIAS DE LA FALTA DE SEGURIDAD EN UNA EMPRESA

Perdidas de información, robo de datos, falta de credibilidad de los clientes y usuarios, impactos económicos y pagos de indemnizaciones, son algunas de las consecuencias mas frecuentes de no poner en practica sistemas y métodos de seguridad, ni del resguardo de los datos.

4. ACTIVIDADES DE EVALUACIÓN

Tome como referencia la técnica e instrumentos de evaluación citados en la guía de Desarrollo Curricular

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento : Conocer las amenazas y posibles vulnerabilidades de seguridad informática de la empresa; así como las buenas practicas para poder mitigarlas. **Evidencias de Desempeño:** Participación en los aportes en Clase **Evidencias de Producto:** Entrega de ejercicios	Cuestionario de evaluación de los temas propuestos en la unidad .	**Custionario**

6. REFERENTES BILBIOGRÁFICOS

editora, E. (2012). Guía práctica informática básica. Macro. Tomado de http://www.ebooks7-24.com.bdigital.sena.edu.co/?il=2828

Arenaza, A. (2006). Informática I. McGraw-Hill Interamericana. Tomado de http://www.ebooks7-24.com.bdigital.sena.edu.co/?il=657

Ibáñez, P. (2018). Informática I. Cengage. Tomado de http://www.ebooks7-24.com.bdigital.sena.edu.co/?il=7696

Valentín López, Gema María. Informática Básica. 2014. Web.

Grau, Jorge E. (20016). Glosario TICs. Tomado de https://www.campus.fundec.org.ar/admin/archivos/TIC%20-%20GLOSARIO%20TICs%20-%202016.pdf

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Carlos Alberto Gomez**	**Instructor**	**Centro de Comercio y Servicios, Regional Cauca**	**3/06/20**

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)	**Carlos Alberto Gomez**	**Instructor**	**Centro de Comercio y Servicios, Regional Cauca**	**7/06/20**	**Actualización**