**CONALEP**

**PLAN DE SEGURIDAD**

Alumnos: José Ramón Vieyra Morales, Fabiola Alejandra Núñez Juárez, Heber Ortiz Martínez, Brenda Guadalupe Izquierdo Rodríguez, Fátima Yazmin Jiménez Vieyra, Víctor Isaías Santillán García, Dulce Nallely Resendiz Alonso.

C:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0299763.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0195384.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmfC:\Archivos de programa\Microsoft Office\MEDIA\CAGCAT10\j0251871.wmf

entrada

Baños



Laboratorio 3



Laboratorio 1

Cafetería

Salónn

Tronco común

Sala audiovisual

Biblioteca

oficinas

Salónes

Salónes

Salón

Baños

Baños

Laboratorio 2

Estacionamiento



Cancha

***SEGURIDAD EN CENTROS DE CÓMPUTO***



Seguridad es el conjunto de normas preventivas y operativas, orientados a neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia, que afecten y lesionen a las personas o los bienes de esta. Algunas medidas de seguridad de un centro de cómputo son:

**La seguridad en el interior**

**Educar a los usuarios**

Algunos reportes han puesto en una gran cantidad de casos la mayor amenaza de ataques al sistema no proviene de fuera, sino que parte desde el interior de la organización.

Una de las mayores ayudas que puede recibir un hacker que intenta infiltrarse en el sistema de una organización consiste en obtener información acerca de Este.

**No confiar (totalmente) en nosotros mismos.**

**Ejecutar solo los servicios imprescindibles.**

En un sistema de alto riesgo es de obligatorio que se ejecute únicamente lo imprescindible.

En sistemas y redes complejas es muy posible que una sola persona (nosotros) hayamos dejado pasar alguna puerta insegura. Mientras más personas verifiquen nuestro trabajo, habrá más probabilidades de que éste adecuadamente realizado.

**Vigilancia.**

**Seguridad en las instalaciones.**

1.-Impartir instrucciones a los asociados de no suministrar información.

2.- Revisar los planes de seguridad de la organización.  
3.- Establecer simples y efectivos sistemas de señales.  
4.- Contar con resguardo de la información que se maneja.

5.- Establecer contraseñas.

6.- Evitar introducir alimentos.

7.- No fumar.

8.- Cada equipo de cómputo debe contar con un regulador de corriente.

9.- Escanear una Memoria antes de introducirla a la computadora.

Ponciano Vega

Ponciano Vega

Salvador Díaz Mirón

Insurgentes

Octavio Paz

CONALEP 128 MOROLEÓN, GTO.

PLAN DE SEGURIDAD

IDENTIFICACIÓN

|  |  |
| --- | --- |
| Folio | Gtlb-01 |
| Objeto | PC de escritorio |

DESCRIPTORES

|  |  |
| --- | --- |
| Recomendaciones aplican para: | Hardware |
| Origen | Interno |
| Breve descripción | Este equipo de cómputo se encuentra en el laboratorio 1 del plantel conalep.  Es utilizado por los alumnos.  Es una ACER VERITON 6800 con un microprocesador Pentium (R) 4cpu 3.20 GHz 3.19GHz, 0.99 GB de RAM |

POLÍTICAS

|  |  |
| --- | --- |
| De operación | La computadora debe estar siempre conectada a su regulador y solo la pueden usar los alumnos |
| De acceso | La computadora debe de contar con contraseña de administrador |
| De protección física | El laboratorio debe estar cerrado para proteger los equipos |
| De recurso humano | No introducir alimentos o bebidas al laboratorio, seguir las normas puestas por los maestros |
| De red y recuso compartido |  |

IMPLICACIONES

|  |  |
| --- | --- |
| Unidades afectadas |  |
| Costo estimado |  |

|  |  |  |
| --- | --- | --- |
| NOMBRE | RESPONSABILIDADES | PUESTO O DEPARTAMENTO |
| Elizabeth García Zavala | Atender a las personas que vengan a ver al director, atender las llamadas telefónicas, la agenda del director y archivar toda la información del conalep. | Secretaria del director |
| Octavio Vargas Soto | Cumplimiento en el reglamento escolar en cuanto a disciplina y certificados, títulos, cedula profesional, otorgamiento de becas, promotor en actividades culturales y deportivas. | Jefe de servicios escolares. |
| Rodolfo Antonio Zavala Vallejo | Cuida que los alumnos estén en clases | Titular escolar y departamento escolar |
| Laura Ortega Valadez | Departamento de capacitación emocional y vinculación, zonas marginadas y centro evaluador | jefe de proyecto |
| Mónica Iveth López Guzmán | Elaboración y revisión de las nóminas docentes y administrativas, registro y control de las operaciones contables y respetables de los ingresos del CONALEP. | Jefe de proyecto de servicios administrativos |
| María de Lourdes Diego Jacob | Realiza los cobros del plantel | Área de caja y secretaria |
| Silvia García Reyes | Sistema de administración escolar SAE; validación de documentos como certificados de estudio, elaboración de título, encargada de becas anteojos, becas media superior y beca de subsidio, servicio social y prácticas. | Subjefe técnico especialista en áreas escolares. |
| María del Refugio | Becas de oportunidades, seguro social y seguro de vida | Servicios escolares |
| Ana Tapia Alcanzar | Atiende la biblioteca, los libros, las credenciales y orienta a los alumnos en las computadoras | Bibliotecaria |
| Graciela Alvares Castro | Captura los sistemas SAE, subjefe MSPS, bajar programas de estudio, horario de clases, archivo y control de asistencia. | Secretaria C |
| Janet López Guzmán | Encargada del taller de industria del vestido. | Área Administrativa |
| Reimundo Luna | Asistir a mi trabajo diario | Jefe de proyectos de información técnica |

|  |  |  |
| --- | --- | --- |
| SOFTWARE | CARACTERITICAS | UBICACION |
| Sistema operativo | Microsoft Windows XP Profesional Versión 2002 Servicie Pack 3 | Equipo Laboratorio 1 |
| Microsoft Office | Microsoft Office Professional Plus2010 | Equipo Laboratorio 1 |
| Antivirus | Avast! Free Antivirus | Equipo Laboratorio 1 |
| Adobe Reader | Lector de documents PDF | Equipo Laboratorio 1 |

**ANALIZA MODELOS Y BUENAS PRÁCTICAS DE SEGURIDAD INFORMATICA:**

**ITIL:** La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL, es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

**Cobit:**

**ISM3:**

**ANALIZA ESTANDARES INTERNACIONALES DE SEGURIDAD**

**BS 17799:** BS 17799 es un código de prácticas o de orientación o documento de referencia se basa en las mejores prácticas de seguridad de la información, esto define un proceso para evaluar, implementar, mantener y administrar la seguridad de la información. El objetivo es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones de confianza entre las empresas.

**Serie ISO 27000:** ISO/ 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

**ISO 27001:** Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO17799).

**ISO 27002:** Es la guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.