CENTRO DE CAPACITACION DON BOSCO

MANUAL DE SEGURIDAD

GEM006

0	Elaboración del Manual de seguridad en las instalaciones de Centro de Capacitación Don Bosco	Luz Adriana Gómez	Comité de Calidad	P. Germán Londoño	05.09.13
REV No.	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**	**FECHA**

Aprobado: _____

TABLA DE CONTENIDO

1. POLITICA DE CONTROL Y SEGURIDAD

Generar confianza, respaldo y seguridad a toda la comunidad educativa pastoral y partes interesadas del Centro de Capacitación Don Bosco y Villa Don Bosco, mediante la implementación y mantenimiento de mecanismos de control y seguridad a nivel interno, con el fin de prevenir prácticas ilícitas y evitar el acceso a personas no autorizadas que afecten el normal desarrollo educativo, las instalaciones, el bienestar de los empleados, estudiantes y el cumplimiento de todas las normas legales requeridas; mediante un compromiso y confidencialidad de toda la organización, generando así una cultura de seguridad y manteniendo nuestra imagen.

1.1 GENERALIDADES

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de laInformación garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas.

Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones de la entidad apoyadas en un correcto sistema de información.

1.2 OBJETIVO

El Manual de Seguridad para el Centro de Capacitación Don Bosco y Villa Don Bosco, tiene como finalidad dar a conocer las políticas y estándares de Seguridad Informática, de acceso, control, recursos humanos y demás aspectos que permitan proteger y conservar adecuadamente los activos tecnológicos y la información de la institución.

Con la promulgación de la presente Política de Seguridad de la Información, la institución formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo.

Se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y Disponibilidad de la información de la institución.

La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite.

La institución deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información se realicen en los tiempos establecidos.

Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento. (Acceso, toma de respaldo, backup, transporte, recuperación, otros).

Los usuarios respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas.

2. ALCANCE

Las Políticas y estándares de Seguridad son de aplicación para todos los usuarios y empleados y cualquiera que sea su condición contractual, con el fin de hacer buen uso, proteger, preservar y administrar la información y servicios de la institución.

3. DEFINICIONES

Acceso: Es el privilegio de una persona para utilizar un objeto o infraestructura.

Acceso Físico: Es la actividad de ingresar a un área.

Acceso Lógico: Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.

Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Contraseña: Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.

Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

4. POLITICAS, NORMAS Y MEDIDAS DE SEGURIDAD-SEGURIDAD INSTITUCIONAL

Toda persona que ingresa como empleado nuevo al Centro de Capacitación Don Bosco y Villa Don Bosco debe aceptar las condiciones de confidencialidad entregadas en la oficina de Gestión Humana.

5. CONTROL DE ACCESOS Y SALIDAS DE LA INSTITUCIÓN

5.1 ENTRADA Y SALIDA DE ESTUDIANTES, DOCENTES Y EMPLEADOS

Para ingresar a los diferentes espacios de la institución, los estudiantes, docentes y empleados administrativos deberán portar de manera visible y/o mostrar su Carnet de identificación personal con fotografía, la cual deberá estar vigente, y deberá mostrarla siempre al personal de vigilancia y/o al funcionario que la requiera.

Los docentes y personal administrativo deben Registrar su ingreso y salida en la Plataforma ubicada en la Recepción. De igual forma, si el permiso obedece a salidas fuera de la institución debe diligenciar el formato de Permiso, el cual debe ir firmado por su jefe inmediato o quien haga sus veces de responsable.

En el caso de los Talleres, el docente se compromete a revisar oportunamente el uso de carnet, documento de identidad y seguro cuando lo amerite.

Cuando un empleado se retire o le sea cancelado su contrato debe hacer entrega del carnet en el área de Recursos Humanos.

Cualquier persona que tenga acceso a las instalaciones, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de portería, el cual podrán retirar el mismo día.

En caso contrario deberá tramitar la autorización de salida correspondiente.

Las computadoras personales, y cualquier activo de tecnología de información, podrán ser retirados de las instalaciones únicamente con la autorización de salida y aprobación de la dirección.

5.2 USO DEL CARNET EMPLEADOS

Todo empleado de la institución deberá portar su carnet de identificación de manera visible.

El área de Recursos Humanos deberá procurar la confección de todos los carnets de identificación de los empleados al momento de ser incorporados a la institución.

El primer carnet le será entregado al empleado, cuyo costo será cubierto por la institución y en caso de deterioro del mismo también le será sustituido.

En caso de pérdida del carnet, el empleado de la institución deberá reportar la misma, y cubrir el costo de la elaboración de un nuevo carnet.

Los empleados deberán registrar su ingreso y salida de la institución en el lector localizado en el área de recepción.

No está permitido prestar el Carnet de identificación a otros empleados o visitantes.

En caso de que algún Directivo, Docente o Funcionario deje de laborar para la institución, el área de Recursos Humanos deberá recuperar el carnet para su anulación. El carnet anulado deberá ser conservado en el archivo correspondiente del empleado.

5.3 ENTRADA Y SALIDA DE VISITANTES.

1. El personal de vigilancia y de recepción, deberán registrar a los visitantes en el formato correspondiente.

2. Se solicitará se identifique el visitante mediante documento oficial, el documento permanecerá en la caseta de vigilancia y/o en la recepción hasta la salida del visitante. Se le hará entrega de un Carne de visitante, el cuál debe ser portado en un lugar visible durante el periodo que dure la visita.

3. El Personal de vigilancia y/o la recepcionista informará al visitante donde se encuentra la persona a quien visita.

4. El anfitrión es responsable del comportamiento de su visitante y de exigirle cumplir con las políticas de control de acceso.

5.4 ENTRADA Y SALIDA DE VEHÍCULOS EN ESTACIONAMIENTOS PARA VISITANTES.

1. Para ingresar al estacionamiento los visitantes deberán identificarse mediante documento oficial.

2. Para poder ingresar al edificio el visitante deberá seguir el procedimiento específico señalado para entrada y salida de visitantes.

3. El servicio de Vigilancia revisará el vehículo al ingreso y salida de la institución.

6. ENTRADA Y SALIDA DE PERSONAS EN AREAS RESTRINGIDAS.

Se considera área restringidas todas las áreas e instalaciones internas de la institución cuyo funcionamiento representa una importancia estratégica significativa para las operaciones diarias, las cuales en caso de ser vulneradas implican un serio daño para la operación e imagen de la Institución.

En tales casos se debe seguir el procedimiento específico para cada caso antes mencionado y aun cuando la persona cuente con un permiso de trabajo debidamente autorizado, el personal de vigilancia, deberá solicitar el apoyo del coordinador general para verificar dicha autorización y el acceso se autorizará siempre y cuando el visitante sea supervisado y/o acompañado por personal de la institución.

Son áreas restringidas: Áreas de Cocina, Bodegas de alimentos, Almacén, archivo general y de los programas de Protección, Tesorería y áreas Administrativas y de dirección.

7. RECEPCIÓN DE CORRESPONDENCIA INTERNA

La correspondencia es recibida por la Recepcionista quien diligencia en el formato GER, la fecha, hora, y la persona q quien va remitido y se distribuye a quien corresponde o se entrega a la tesorería cuando es información administrativa o directiva.

Si llegan paquetes o entregas de mayor volumen se avisa directamente a quien corresponde o de ser material del almacén se entrega directamente en esta área.

8. CUSTODIA, ENTREGA Y RECEPCIÓN DE LLAVES

El área Administrativa cuenta con un casillero para la custodia de las copias de llaves de cada una las oficinas y talleres, estas llaves sólo son autorizadas y manejadas por el Ecónomo y Auxiliar de archivo en su ausencia; quien entrega y recibe las llaves en caso de pérdida o extravío de las llaves en el momento que le fueron entregadas.

En Recepción, reposan las llaves de talleres, salones, los cuáles son entregados al docente titular, quien firma la planilla de entrega y devolución de estas al final de la jornada. En ausencia de la Recepcionista son dejadas en custodia del vigilante de turno.
A partir de la entrega de las llaves, el responsable será el usuario solicitante hasta su devolución.

9. SEGURIDAD INFORMATICA

9.1 REDES SOCIALES (Facebook, YouTube, Flicker, Twitter, etc)

- Las redes sociales oficiales de la institución serán administradas por el área de Comunicaciones.
- Los grupos o cuentas de las redes sociales para la Institución deben ser creadas por el área de Comunicaciones, el manejo de las mismas se delega a cada área, que solicite el manejo de la cuenta.

9.2 PUBLICACIONES EN LA PÁGINA PRINCIPAL DEL SITIO WEB

- El área de Comunicaciones es el único ente que podrá publicar información en este espacio del sitio web y panel de noticias.

- Si algún área necesita publicar información en este espacio deberá tramitarla al área de Comunicaciones con el respectivo archivo o información a publicar.

9.3 CONTROL DEL CORREO INSTITUCIONAL

NORMAS Y DEBERES:

- La identificación de los servicios informáticos es única y exclusivamente para uso personal, para actividades netamente institucionales y deberá ser empleada únicamente por la persona a quien le fue asignada. El correo es de uso personal e intransferible.

- Es deber de cada usuario asegurarse de cerrar la sesión de trabajo una vez finalice la utilización de todos los servicios a fin de que nadie más pueda utilizar su identificación. El olvidar esta tarea puede acarrear graves consecuencias para el usuario, que van desde la posibilidad de pérdida de información y el envío de correos a su nombre, hasta el uso inadecuado, por parte de otras personas, de los recursos que le fueron asignados.

- Si un usuario encuentra abierta la identificación de otra persona es su deber cerrarla y por ningún motivo deberá hacer uso de ella.

- Toda comunicación oficial se deberá realizar a través del correo institucional con dominio ccdonbosco.org según corresponda.

- El usuario será el único responsable del perjuicio que pueda llegar a ocasionarle el no poder enviar ni recibir mensajes y archivos de correos electrónicos en caso de que el espacio que se le haya asignado este agotado.

- El usuario de correo institucional debe revisar con frecuencia el buzón de su cuenta de correo.

- No se debe realizar envío de correos tipo cadena o forwards desde los correos corporativos con información que no pertenezca a la comunidad académica o institucional.

POLÍTICAS DE USO:

- Cada buzón de correo tendrá una capacidad de acuerdo a lo que designe el proveedor del servicio de correo electrónico.

- La Institución no se hace responsable por el contenido de texto, sonido, video o cualquier otro que el usuario envíe o reciba usando el correo electrónico institucional.

- En el momento en que el usuario deje de ser empleado de la institución se cancelará en forma inmediata el servicio de Correo Electrónico; la institución no se hace responsable de pérdidas de información por este proceso. En caso de reingreso, la institución no puede asegurar la disponibilidad del mismo nombre de usuario ni mucho menos del backup de los archivos del periodo anterior.

- Mantener y ejecutar funciones de administración para eliminar aquellos mensajes que no requieran estar almacenados con el fin de mantener espacio disponible tanto para enviar como para recibir nuevos mensajes.

- Es deber de los usuarios, cada vez que se identifiquen con una cuenta de correo Institucional, velar porque no se comprometa la buena imagen de la institución.

Todos los archivos de computadoras que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

10. RESPALDO Y BACKUPS DE INFORMACIÓN

El área de Sistemas realiza Backups con una regularidad de una vez al mes, no obstante cada unidad, área o departamento es responsable de hacer copias de su información.

11. MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE:

Esta actividad se desarrolla de acuerdo con la elaboración previa de un cronograma aprobado por la dirección, el cual se socializa a través de correo electrónico a todos los funcionarios.

Únicamente el personal autorizado por el área de Sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

12. PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del encargad de activos fijos.

El Área de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Queda terminantemente prohibido que el usuario o funcionario distinto al personal del área de Sistema abra o destape los equipos de cómputo.

Todo funcionario responsable de equipos informáticos debe dejarlo apagado y desenchufado para ahorrar recursos energéticos y contribuir a la conservación de los equipos y del medio ambiente. De igual forma, apagar los monitores o poner en modo de ahorro si va a salir de la oficina por espacios cortos.

Abstenerse de realizar el préstamo de su equipo (Herramienta de trabajo necesaria para el cumplimiento de sus funciones) a Aprendices, familiares o cualquier persona que no tenga relación con actividades laborales de la institución.

En lo referente al uso de memorias, dispositivos (cámaras, teléfonos) si esta se utiliza en equipos poco confiables por favor realizar el examen de análisis del dispositivo en la sala de sistemas 4 antes de utilizarlo en un equipo de la institución.

13. ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO

Los usuarios y funcionarios que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

Los usuarios y servidores deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

El control de manejo para las licencias y el inventario de los será responsabilidad del área de Activos Fijos.

14. INTERNET

El acceso a Internet provisto a los usuarios y funcionarios es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

Los usuarios del servicio, tienen prohibido el acceso a páginas no autorizadas, con material pornográfico o de contenido ilícito o que estén por fuera del contexto laboral.

No se permite la descarga de software, videos, música y reproducción de videos que no tengan que ver con el proceso formativo, sin la autorización de los encargados del área de Sistemas con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.

El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo al área de Sistemas que se encargará de realizar las operaciones oportunas.

Como medida de seguridad si realiza tareas institucionales fuera de la institución es conveniente utilizar herramientas de la nube tales como Google drive, Dropbox, etc que permiten guardar o descarga la información con seguridad en los equipos de la institución.

Igualmente para seguridad en el uso de la **Red Wifi**, se ha dispuesto el cambio periódico de las claves de acceso, las cuales solo podrán ser comunicadas al persona que lo requiere y que se ha definido desde la Dirección de la institución para su conocimiento y manejo, por favor abstene

rse de solicitarlas sino cuenta con la autorización respectiva, y de estar autorizado se solicita total reserva de esta información

15. ACCESO LOGICO

15.1 CONTROLES DE ACCESO LÓGICO

Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga la aprobación de la dirección.

15.2 ADMINISTRACIÓN Y USO DE CONTRASEÑAS

La asignación de contraseñas debe ser realizada de forma individual, lo que el uso de contraseñas compartidas está prohibido.

Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al área de Sistemas para que se le proporcione una nueva contraseña.

Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos

Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.

Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10).Estos caracteres deben ser alfanuméricos, o sea, números y letras
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario; y
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

Para el área de Contabilidad y los Equipos que tengan instalado el Software contable SIIGO su clave deberá ser cambiada cada 30 días y comunicada al dueño del proceso.

15.3 CONTROL DE ACCESOS REMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por la dirección.