MANUAL DE PROCEDIMIENTOS DE LA ACTIVIDAD DE INFORMÁTICA

INDICE

Contenido

TITULO: MANUAL DE PROCEDIMIENTO DE LA ACTIVIDAD INFORMATICA

REV. _____	ELABORADO	REVISADO	APROBADO
NOMBRE	OSMANY FERNANDEZ	LORENA CERNA	
CARGO	JEFE INFORMATICA	PRESIDENTA FUNDACION	
FIRMA			
FECHA	15/04/2024		
PAGINAS REVISADAS: 45			

REV. _____	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

PAGINAS REVISADAS:

REV. _____	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

PAGINAS REVISADAS:

REV. _____	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

PAGINAS REVISADAS:

REV. _____	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			
PAGINAS REVISADAS:			

Procedimiento # 1 Sistema Control de Acceso a los Locales.

Objetivo: Regular el acceso a los locales donde se encuentran las tecnologías informáticas, para que no accedan personal no autorizado a las tecnologías informáticas y departamentos.

Alcance: Todas las áreas con TIC que están comprendidas en las áreas del colegio y todas las personas pertenecientes o no a nuestra entidad, que por cualquier motivo accedan a nuestras tecnologías.

Desarrollo:

- Los jefes de las Áreas son los responsables del personal con nivel de acceso a los locales bajo su dirección.
- Las Áreas limitadas tendrán una relación del personal con nivel de acceso al local en un documento con los siguientes datos:
  - Nombre del Área:
  - Cargo de la persona autorizada:
  - Firma del máximo directivo de la entidad:
  - Nombre del máximo directivo de la entidad:
  - Cuño encima de la firma del máximo directivo de la entidad:
  - Quedará plasmado en la puerta de acceso al local.
- La Gerencia autorizará la entrada a los locales de personal ajeno a la empresa y se realizará siempre en presencia de una persona con nivel de acceso autorizado.
- El nochero comprueba después de las 18:00 horas la seguridad de los locales del colegio, así como las puertas laterales y traseras del edificio. La puerta principal la mantendrá abierta o cerrada de acuerdo con su consideración, velando siempre que guarde las medidas de seguridad del nivel de acceso.
- Las salas y todos los locales deben permanecer cerrados y sellados una vez concluida la jornada escolar y el aseo de las mismas, registrando en un libro de incidencia como se encontró el edificio para la noche.
- Todas las personas ajenas al colegio que deseen por una u otra razón ingresar al colegio, se le entregará en portería un solapín que identificará el propósito de su estancia.
- El personal ajeno al colegio no puede bajo ningún concepto ingresar a locales sin la presencia de un Jefe de área o trabajador que este designe para ello.

Procedimiento # 2 Sistema de Control de los bienes Informáticos.

a) Clasificación e identificación de los Medios Informáticos.

Objetivo: Clasificación e identificación de los Medios informáticos.

Alcance: Todos los bienes informáticos de nuestra entidad.

Desarrollo:

Se consideran Medios informáticos todos los equipos, útiles y materiales utilizados en el aseguramiento de la actividad informática, los que se agruparan en las siguientes categorías:

- Equipos Informáticos (Activos Fijos Tangibles)
- Partes y Piezas de Equipos Informáticos
- Útiles y Herramientas de Computación.
- Materiales e Insumos de Computación (Materiales)

Los Medios Informáticos que se deben conceptuar como Activos Fijos Tangibles son los siguientes:

- Servidores y Computadoras
- Monitores
- Impresoras
- Ploteadores
- Escáneres de mesa y digitalizadores.
- Videoproyectores (Data Show).
- Cámaras Digitales.
- Fuentes de alimentación interrumpibles (UPS) de menos de 3 KVA, estabilizadores y transformadores asociados a equipos informáticos.
- Conmutadores (Hubs, Switchs y Data Switch).
- Dispositivos de transmisión de datos: módems y fax-modem externos, transceivers, equipos de radioenlace y otros de similares funciones.
- Gabinetes (racks) para el montaje y protección del equipamiento activo de redes.
- Fuentes interrumpibles de alimentación (UPS) de 3 o más KVA para sistemas centralizados de fuerza.
- Equipos de sonido.

Los Medios Informáticos para conceptuar como Partes y Piezas son:

- Tarjetas y bloques de circuitos para computadoras y periféricos.
- Discos duros internos.
- Chips: memoria, microprocesadores y otros.
- Dispositivos internos de lectura y grabación de información, lectores o quemadores de discos compactos o de discos versátiles (DVD).
- Módems y fax-modem internos.
- Chasis de equipos informáticos con o sin fuente de alimentación.
- Fuentes de alimentación internas para equipos informáticos.
- Cabezales, inyectores, fusores y rodillos para equipos de impresión.
- Lámparas para Video proyectores y escáneres.
- Equipos de sonido. (subwoofer).

Los Medios Informáticos que deben ser tratados como útiles son:

- Herramientas de computación.
- Maletines (carrying case) para equipos informáticos.
- Dispositivos externos de salva de información

Los Medios Informáticos para conceptuar como materiales (insumos) son:

- Dispositivos de control y de entrada de datos; teclados, ratones, bastones de mandos (joysticks), escáneres de mano y otros de funciones similares.
- Parlantes o Altavoces.
- Cargadores de baterías y adaptadores DC/AC para equipos informáticos.
- Papel de forma continua.
- Discos compactos y versátiles; CD-R, CD-RW y DVD.
- Cartuchos de tinta y tóner para impresoras.
- Cintas para impresoras.
- Cintas y cartuchos para dispositivos de salva.
- Baterías para UPS, computadoras y otros equipos informáticos.
- Materiales para limpieza, mantenimiento y reparación de equipos informáticos.
- Teclas, botones y bandejas.
- Cables y conectores.
- Mouse.

b) Sistema de Reparaciones, Mantenimientos y Modernización de los Medios Informáticos.

Objetivo: Control sobre las reparaciones, mantenimientos y modernizaciones de los medios informáticos.

Alcance: Todos los bienes informáticos de nuestra entidad.

Desarrollo:

Reparaciones

- La reparación al equipamiento informático se realizará en primer lugar por el departamento informático del colegio, el cual determinará con previa autorización de la Gerencia, si es necesario el traslado hacia una empresa especializada debido a la complejidad del asunto y el uso de herramientas específicas. En tal sentido se establecerán contratos puntuales para la ejecución de un trabajo o facturas electrónicas a decisión de la Gerencia.
- La asistencia técnica al equipamiento que se encuentre comprendido entre los términos de su garantía comercial se asegurará por la entidad que haya definido el proveedor para este servicio.
- El departamento Informático podrá realizar reparaciones menores al equipamiento informático instalado en su unidad utilizando partes y piezas adquiridas por el presupuesto aprobado.
- Durante la reparación de un equipo fuera del término de su garantía comercial se procederá a la sustitución de determinadas partes y piezas de este, estas deberán ser entregadas como chatarra electrónica a una empresa especializada en el tema, mediante documento que sea firmado por ambas partes y aprobado por la Gerencia o, en su defecto, la empresa reparadora certificará mediante documento su apropiación de las partes y piezas sustituidas.
- Se considerará una reparación capital aquella que implique la sustitución de un 80% o más de las partes y piezas de un equipo con el objetivo de restablecer totalmente sus capacidades tecnológicas esenciales.

- Se admitirá la realización de una reparación capital sólo cuando el costo de esta sea inferior o igual a la adquisición de un equipo nuevo de características similares.
- El departamento informático informará al área de contabilidad, cuando se realice una reparación capital de un equipo informático conceptuado como activo fijo para modificar su valor actual en un monto equivalente al valor de las piezas utilizadas para restablecer su capacidad técnica. Esta acción no modificará el número de inventario como activo fijo.
- En caso de que un equipo sea reparado por una empresa de asistencia técnica, está emitirá órdenes de servicios y (o) facturas electrónicas donde se haga constar las partes y piezas que fueron objeto de reparación y la fecha de su realización, las cuales serán archivadas en un expediente del área contable con copia en el expediente del equipo.
- El Departamento Informático firmará la orden de servicio como constancia de realización del trabajo.
- Las partes y piezas en buen estado que se recuperen como resultado de una reparación se controlaran por el encargado del departamento Informático. Estas partes y piezas podrán ser utilizadas para la reparación de otros equipos sin modificar su valor actual.
- Las partes y piezas rotas que se recuperen como resultado de una reparación se controlará por el encargado del departamento Informático y se registraran en el Listado de Partes, Piezas y Útiles de Computación Defectuosos para gestionar su baja.
- Toda reparación que se ejecute a un equipo debe ser registrada en el Expediente técnico digital del mismo.

Mantenimiento

- La frecuencia con que se efectuará el mantenimiento al equipamiento informático no debe ser por un periodo que exceda los 12 meses, por lo que se debe dar 1 mantenimiento como mínimo al año.
- El mantenimiento informático se realizará por el departamento informático con medios propios, se podrá proceder a ello mediante la adquisición de los insumos y herramientas requeridos por el presupuesto aprobado.
- El departamento informático solicitará el servicio de mantenimiento a la empresa de asistencia técnica con la cual se tiene contrato de mantenimiento.
- El departamento informático reflejará en el Expediente técnico digital del equipo la acción realizada, siendo esta certificada por el encargado del departamento.

Modernizaciones

- Las modernizaciones serán aplicadas sólo a las computadoras y servidores.
- Las modernizaciones se realizarán con el objetivo de mejorar las prestaciones de una computadora o servidor cuyas capacidades tecnológicas no se correspondan ya con las requeridas por el puesto de trabajo donde la misma es utilizada o para alargar la vida útil de un medio tecnológicamente envejecido.
- La modernización sólo se podrá realizar cuando su costo sea inferior al de adquirir un equipo nuevo con prestaciones similares a las que se obtendrían como resultado de esta.
- La modernización se realizará por una empresa especializada o por el departamento informático.
- El Departamento Informático informará a Gerencia cuando se realice una modernización de una computadora o servidor para incrementar su valor actual en un monto equivalente al valor de las partes y piezas utilizadas. Esta acción no modificará el número de inventario como activo fijo.
- Las partes y piezas en buen estado que se recuperen como resultado de una modernización se controlarán por el Departamento Informático. Estas partes y piezas podrán ser utilizadas para la reparación de otros equipos sin modificar su valor actual.
- Las partes y piezas rotas que se recuperen como resultado de una modernización se controlará por el Departamento Informático y se registrará en el Listado de Partes, Piezas y Útiles de Computación Defectuosos.

Anexos: Expedientes de los computadores.

c) Sistema de Control físico de los Medios Informáticos.

Objetivo: Controlar físicamente los medios informáticos.

Alcance: Todos los bienes informáticos de nuestra entidad.

Desarrollo:

Control físico del equipamiento informático

- El Departamento Informático asegurará la confección y permanente actualización de los siguientes documentos para el control físico del Equipamiento Informático.

  Tabla de Equipamiento Informático: Se realiza mediante una plataforma digital

  Expediente técnico digital. (Libro de Control de Reparaciones).

- La **Tabla de Equipamiento Informático** se controla a través del Sistema de Solicitudes de Tecnologías, donde se recogerán las características esenciales de servidores, computadoras y todos los medios asociados al departamento informático del colegio.
- En la Tabla de equipamiento informático se recogerán los datos de todos los equipos existentes en la unidad, se encuentren o no en explotación existiendo una correspondencia exacta entre los medios consignados en dicha tabla y los que se encuentran registrados como activos fijos.
- El **Expediente técnico digital** es un registro de control que forma parte del sistema de solicitudes de tecnología y se mantendrá actualizado por el Departamento Informático de forma individual por cada configuración de servidor, computadora. Este expediente se mantendrá asociado a cada equipo desde el momento de su adquisición hasta el momento en que se produzca su baja técnica y en el mismo se dejará constancia permanente de los diferentes elementos que conforman dicha tecnología, así como de todos los cambios que se ejecuten sobre la misma como resultados de las acciones de reparación, modernización y sustitución de dispositivos.
- El Departamento Informático mantendrá restringido los permisos de acceso a los Expedientes Técnicos de los equipos informáticos de la entidad, el cual será el único autorizado para hacer las anotaciones y registros en los mismos.

- Los datos consignados en el Expediente técnico digital de un equipo informático deben corresponderse con la situación real del mismo y será certificado por el Jefe del departamento informático.
- El **Libro de Control de las Reparaciones** es un documento de registro que se habilita por el departamento informático para registrar las acciones de reparación que se ejecuten sobre otros equipos informáticos o de redes. Este se encuentra dentro del Expediente técnico digital.

Control físico de las Partes, Piezas, Dispositivos, Herramientas y Accesorios de Computación.

- El Departamento Informático asegurará la confección y actualización de los siguientes documentos para el control físico de las Partes, Piezas, Dispositivos, Herramientas y Accesorios de Computación: Expediente técnico digital.
- Las Partes y Piezas adquiridas para asegurar la reparación, modernización o ampliación de capacidades del equipamiento informático instalado en el colegio sólo podrán ser entregados al Departamento Informático para su utilización controlada con estos fines.
- El Departamento Informático mantendrá actualizado el Expediente técnico digital donde se registrará, tantos las partes y piezas nuevas que le hayan sido entregadas para la ejecución de reparaciones, modernizaciones y ampliaciones, como aquellas en buen estado que hayan sido sustituidas en cualquier equipo y que puedan ser utilizadas posteriormente.
- Las partes y piezas en mal estado técnico que hayan sido reemplazadas en cualquier equipo se controlarán por el Departamento Informático mediante su inclusión en el Listado de Partes, Piezas y Útiles de Computación Defectuosos.
- La sustitución de una parte o pieza que se realice a una computadora o servidor, así como a cualquier equipo informático se registrará por el Departamento Informático en el Expediente técnico digital o en el Libro de Control de Reparaciones, según corresponda.
- Todo dispositivo o herramienta de computación cuyo deterioro lo haga inservible será entregado al Departamento Informático, realizando su inclusión en el Listado de Partes, Piezas y Útiles de Computación Defectuosos.

Anexos

- Expediente técnico digital

d) Sistema de Control de los movimientos Informáticos.

Objetivo: Controlar los movimientos de los medios informáticos en los locales de la unidad.

Alcance: Todas las áreas con activos informáticos del colegio

Desarrollo:

- La Gerencia del centro es quien autoriza todo cambio de un medio informático en su área y con la previa coordinación del Encargado de la Actividad Informática a fin de garantizar la adecuada actualización del Expediente técnico digital.
- El cambio de ubicación de un medio informático entre áreas de nuestro colegio podrá realizarse sólo con la autorización de la Gerencia y previa coordinación con el Encargado de la Actividad Informática a fin de garantizar la adecuada actualización del Expediente técnico digital. Cuando el medio esté conceptuado como un Activo Fijo se aplicarán los procedimientos establecidos para los movimientos de medios básicos.
- La extracción temporal de un medio informático para la realización de trabajos o el aseguramiento de actividades fueras de las mismas por el personal propio deberá ser autorizado por la Gerencia del colegio.
- Cuando un medio informático conceptuado como Activo Fijo tenga que ser trasladado a un taller para su reparación se confeccionará para el mismo, los documentos establecidos para movimientos de medios básicos. El Encargado de la Actividad de Informática realizará las actualizaciones necesarias en el Expediente técnico digital o en el Libro de Control de las Reparaciones, según corresponda, una vez que el mismo sea devuelto por el taller.

Anexos

- Expediente técnico digital.

e) Sistema de Control de las Bajas de los bienes informáticos.

Objetivo: Controlar las bajas de los medios informáticos.

Alcance: Todos los bienes informáticos de nuestra entidad.

Desarrollo:

- El dictamen técnico que avala el estado de cada equipo propuesto para baja y la imposibilidad de su utilización debe contar con la certificación del Departamento Informático, el grupo directivo y la Gerencia del colegio. Si fuese preciso y solicitado por la Gerencia, también contará con la alegación de una empresa especializada en el tema.
- Las partes y piezas en buen estado técnico de una computadora o servidor que, en correspondencia con el dictamen técnico elaborado, se proponga como baja y que se considere pueden ser utilizadas para la reparación de otros equipos similares serán retiradas de la configuración, realizando las anotaciones correspondientes en el Expediente técnico digital.
- Las partes y piezas en buen estado técnico de otros tipos de equipos informáticos propuestos a baja podrán ser eventualmente utilizadas para la reparación de otros equipos similares, siempre y cuando esta reparación se ejecute por el Departamento Informático, realizando las anotaciones correspondientes en el Expediente técnico digital.
- Al solicitar la baja de los equipos informáticos hará llegar a la Gerencia y con previa revisión por el Departamento Informático, un Expediente de Baja conformado por los siguientes documentos:
    - Relación de equipos propuestos para Baja, la que se confeccionará como una tabla única donde se consignen los datos generales de todos los medios.
    - Modelo de Baja de los Equipos Informáticos, dictamen técnico de la entidad especializada que certifica el estado del medio y modelo de movimiento del Activo Fijo (propuesto para baja técnica), los que se elaboraran para cada equipo.

Este Expediente de Baja se presentará por el departamento informático en una carpeta donde se incluyan todos los documentos antes relacionados debidamente ordenados.

Anexos

- Expediente técnico digital.

Procedimiento # 3 Sistema de control de entrega y uso de las tecnologías

a) Control de acceso a la tecnología informática.

Objetivo: Regular el acceso a las tecnologías informáticas instaladas y las de uso móvil.

Alcance: Todos los locales donde exista o usen las Tecnología informáticas.

Desarrollo:

- Se velará porque la carga de los equipos esté apta para suplir las solicitudes que se envían para el proceso docente y en su defecto se identificará en el registro la causa para evitar que ocurra nuevamente.
- La entrega de los equipos (notebook, tablet o PC de escritorio) se hará directamente al docente, bajo ningún concepto podrá recibir la tecnología un alumno.
- Las solicitudes de tecnologías para proceso docente o cualquier otro evento, deben hacerse a través de la plataforma que implemente el colegio.
- Las tecnologías serán preparadas con anticipación y se tendrán listas para su uso para no afectar el tiempo requerido, por lo que es preciso que se cumpla con las solicitudes y el horario reflejado en la misma, el no cumplimiento de esto puede afectar el proceso docente. De no poder ejecutar la solicitud, informar personalmente y con anterioridad al departamento de informática.
- Las tecnologías podrán usarse en las salas y deben ser retiradas por el docente en la sala de informática.
- En el caso específico de la biblioteca los notebooks deben ser entregados por números de lista y finalizado el turno, el docente debe proceder a retirarlos y almacenarlos en el rack donde se cargan.

- Las tecnologías cuentan con un número de serie para su identificación que van del 01 al 35 para que sean entregados a los estudiantes según su número de lista.
- Se retirarán las tecnologías una vez culminado el horario indicado, teniendo en cuenta la planificación que se generó en la página, logrando así que cada curso disfrute del tiempo que programó y del equipo en óptimas condiciones.
- Durante el uso de las tecnologías es responsabilidad del docente, asistente o administrativo que lo solicitó, el cuidado y buen manejo de los equipos, en aras de conservar la disponibilidad y su funcionalidad.
- El laboratorio se mantendrá disponible para los estudiantes desde las 8:15 horas hasta 16:15 horas y será ocupado según el calendario de solicitudes. Este contará con un registro de acceso y reglamento escolar.
- El laboratorio de los docentes estará disponible durante toda la jornada laboral, permaneciendo cerrado mientras ningún docente lo ocupe. Cada computador contará con un registro donde se recogerá información necesaria para dar seguimiento al uso del equipo.
- Los equipos se revisarán cada vez que culmine un curso siempre y cuando no interrumpa el proceso docente y se llevará un registro para cada tecnología.

INSTRUCTIVO

SOLICITUD Y USO DE TECNOLOGÍA

1. Para solicitar y utilizar la(s) tecnología(s) del colegio se debe realizar a través del calendario en plataforma https://saintpatricktemuco.cl/tecnologia/calendario.php

Uso de la sala de computación

1. Para solicitar y utilizar la sala de computación del colegio, se debe realizar la solicitud a través del calendario en plataforma https://saintpatricktemuco.cl/tecnologia/calendario.php
2. El encargado de computación abrirá la sala de acuerdo con el horario solicitado y usted deberá cerrar una vez terminadas sus actividades.
3. Sí quien solicita la sala de computación se atrasa en el horario acordado, el encargado de computación puede no estar disponible para abrir, por lo cual, quien solicitó la sala deberá acercarse a Gerencia a buscar la llave.
4. Se prohíbe el ingreso y consumo de alimentos o bebidas en la sala de computación.
5. Utilizar equipos según número de lista de estudiantes.
6. Velar por el cuidado de los equipos.
7. No mover ningún componente del lugar donde se encuentra ubicado.
8. Mantener la disciplina para evitar daños físicos a los equipos.
9. Mantener las mesas y sillas organizadas y alineadas.
10. Dejar computador encendido.
11. Mantener y cuidar la limpieza de la sala durante el período de uso.
12. Informar de inmediato a encargado de Informática si detecta alguna falla en la tecnología que recibió.
13. Es responsabilidad de quien recibe tecnologías la reposición del medio en caso de falla por fuerza mayor o externa (Ej: Daños físicos, software o extravío del medio).
14. Informar de inmediato cualquier incidente detectado.

CORRECTO USO DE LA TECNOLOGÍA EN SALA DE CLASES

Para llevar a cabo y dar un correcto uso de la tecnología del colegio, usted debe:

1. Cautelar el buen uso de la tecnología dentro del aula.
2. Dejar ordenado el notebook que está a su disposición en sala.
3. Dejar abierto y encendido el notebook (remotamente se actualizará, por lo cual, no debe ser apagado).
4. Velar por la carga del notebook y conectar a la energía eléctrica cuando necesite carga
5. Apagar el televisor al término de cada clase y/o si ya no se está utilizando.
6. Apagar el data. Las lámparas de los proyectores vienen con horas de vida, sí usted lo deja encendido y no lo está utilizando está gastando vida útil del equipo.
7. No sacar tecnología de la sala tales como: controles, cables, notebook, mouse, tablets, etc.
8. No permitir que los alumnos manipulen los televisores, ni otra tecnología sin supervisión y autorización del encargado en sala en ese momento.
9. Retirar las *tablets* en oficina de Informática y revisar que se encuentre organizados por número de identificativo.
10. Devolver los *tablets* organizados por número identificativo tal cual debieron ser entregados.
11. Entregar *tablets* a estudiantes por número de lista.
12. No retirar ni remover protección de los tablets y etiquetas con identificación de números.
13. Cautelar el buen uso de la tecnología dentro del aula.
14. Informar de inmediato a encargado de Informática si detecta alguna falla en la tecnología que recibió.
15. Es responsabilidad de quien recibe tecnologías la reposición del medio en caso de falla por fuerza mayor o externa (Ej: Daños físicos, software o extravío del medio).
16. Los recursos ubicados en sala son responsabilidad del profesor jefe, por lo que debe cautelar el buen uso y cuidado.
17. Informar de inmediato cualquier incidente detectado.

Anexos

- Expediente técnico digital.
- Acta Entrega.
- Registros de control.

Procedimiento # 4 Sistema de Sellaje de Computadoras.

Objetivo: Sellar las computadoras para su protección contra alteraciones o sustracciones.

Alcance: Todas las computadoras de nuestro colegio.

Desarrollo:

- El Encargado de la Actividad informática es el responsable de sellar todas las computadoras del colegio, cada vez que se haga esta acción se reflejará en el Expediente técnico digital.

- El usuario que opera el computador velará porque su ordenador esté debidamente sellado y se indicará en el Expediente técnico digital (Registro de Incidencia) las razones por las que fue cambiado.

- Los usuarios a cargo de los computadores son los máximos responsables de informar al Encargado de la Actividad Informática de cualquier anomalía en el sello de su ordenador.

Anexos

- Expediente técnico digital.

Procedimiento # 5 Sistema de Entrega de Pendrive USB o disco extraible

Objetivo: Controlar las entregas de Pendrive USB a los directivos y administrativos del colegio.

Alcance: Todos los directivos y administrativos del colegio.

Desarrollo:

- El directivo o administrativo solicitará al Departamento Informático la adquisición del Pendrive USB, la cual será aprobada por la Gerencia del colegio.

- La Gerencia aprobará su compra si el directivo o administrativo lo requiere para el desempeño de sus funciones.

- El Departamento Informático entregará mediante acta la Pendrive USB al directivo o administrativo.

- El Encargado de contabilidad llevará a útil la Pendrive USB.

Procedimiento # 6 Perdida o Extravío de Equipos Informáticos.

Objetivo: Controlar las pérdidas o extravíos de equipos, soportes o medio informático con capacidad de almacenar grandes volúmenes de información de nuestro colegio.

Alcance: Todos los equipos, soportes o medio informático con capacidad de almacenar grandes volúmenes de información.

Desarrollo:

- El usuario a cargo de la tecnología debe informar al encargado del Departamento Informático, la pérdida o extravío de la tecnología.
- El encargado del Departamento Informático, a la Gerencia.
- La Gerencia aplicará las medidas correspondientes al responsable del hecho, así como su responsabilidad material según corresponda.
- El Encargado de la Actividad Informática actualizará el Expediente técnico digital del equipo.

Anexos

- Expediente técnico digital.

Procedimiento # 7 Trazar los pasos durante la Alta, Baja o Traslado de usuarios.

Objetivo: Establecer pasos a seguir para la creación de la cuenta de usuario.

Alcance: Todos los usuarios del dominio.

Desarrollo:

Alta del usuario en el Directorio Activo.

- El Departamento informático mantendrá actualizado el Active Directory según la incorporación de trabajadores o traslado de áreas.
- En el Active Directorio estará definido las unidades organizativas que corresponderán a cada área, creando grupos que permitan identificar los diferentes departamentos.
- El encargado de Recursos Humanos incluirá dentro las responsabilidades laborales las funciones y responsabilidades de seguridad informática.
- El Administrador de Red procederá a la creación de la cuenta de usuario y habilitará los derechos y permisos concedidos por el encargado del Departamento y aprobación de la Gerencia.

Baja de usuario en el Directorio Activo.

- El encargado de Recursos Humanos informa de manera oficial al encargado del Departamento Informático, la baja o traslado de todo trabajador, con no menos de 72 horas antes su efectividad.
- El Departamento Informático procederá a cerrar la cuenta de usuario y la inhabilitación de todos los demás derechos y permisos.
- El Departamento informático mantendrá actualizado el Active Directorio según baja de trabajadores o traslado de áreas.

Procedimiento # 8 Sistema Control de Acceso a las tecnologías de la información.

a) Control de acceso a la tecnología informática.

Objetivo: Regular el acceso a las tecnologías informáticas instalada.

Alcance: Todos locales donde se ubica la Tecnología informática.

Desarrollo:

- Procedimiento de Alta, Baja o Traslado de usuarios.
- El Departamento de Informática dará con previa autorización de Gerencia, los derechos y permisos que tienen los usuarios para utilizar las tecnologías e información de su departamento.
- El acceso a la tecnología del personal técnico especializado para la reparación o mantenimiento de la tecnología será autorizado por el Departamento de Informática, siempre realizará sus labores en presencia de una persona con nivel de acceso autorizado a las tecnologías objeto de reparación o mantenimiento.
- El personal interno o externo a la entidad no incluido en la relación autorizada podrá tener acceso a las tecnologías informáticas instaladas en el área, mediante previa autorización del encargado de Departamento Informático (si se trata de personal interno) o Gerencia si se trata de personal externo.
- Las personas ajenas a nuestra entidad que por necesidades de trabajo necesiten usar la tecnología informática y sean autorizado por la Gerencia, siempre estarán acompañados de una persona con nivel de acceso autorizado a la tecnología a utilizar.
- La Gerencia aplicará sanción al personal que haga acceso a las tecnologías y servicios sin estar autorizado.

b) Activación y Control de claves de acceso a las aplicaciones informáticas.

Objetivo: Establecer el procedimiento de activación y compartimentación de las claves de acceso a las aplicaciones informáticas.

AIcance: Todas las aplicaciones informáticas que se encuentran en el dominio del colegio.

Desarrollo:

- La Gerencia determinará los usuarios que estarán autorizado para acceder a las aplicaciones informáticas del colegio, con el nivel de permiso según sus funciones. El Departamento de Informática se ocupará de mantener actualizado el tema.
- El usuario cambiará su contraseña cada vez que estime conveniente.
- Las claves de sesión y correos serán personales e intransferibles.
- Las claves de los controladores de dominio y red, wifi y bluehost, serán de acceso limitado al Departamento de Informático, según determine la Gerencia. Esta contará con un respaldo de todas las contraseñas debidamente actualizado.
- El Departamento Informático mantendrá actualizado el registro de contraseñas, modificando las mismas según se requiera y con previa autorización de la Gerencia.

Procedimiento # 9 Incidentes de la Seguridad Informática.

Objetivo: Gestionar los Incidentes de la Seguridad Informática en el colegio.

Alcance: Todas las áreas con tecnología Informática del colegio, así como todos los usuarios autorizados a usar las TIC.

Desarrollo:

- Al detectar una violación de la Seguridad Informática se debe comunicar al Jefe de Área y este de inmediato dar parte a la Gerencia de la institución.
- El grupo directivo y el jefe del área informática, dirigidos por la Gerencia analizarán los hechos para tomar las medidas pertinentes.
- El jefe de informática recolectará y preservará las trazas del incidente detectado.
- El jefe de informática implementará medidas para prevenir la recurrencia del hecho si fuese necesario.
- Los involucrados directamente en el hecho deben permanecer sin acceso a las tecnologías.
- El área de informática anotará el hecho en el Registro de Incidencia de la tecnología afectada.
- Los equipos informáticos que sufrieron daños permanecerán en cuarentena.

Anexos

Expediente técnico digital.

Procedimiento # 10 Autorización de Uso de Programas de monitoreo en la red de datos.

Objetivo: Controlar el uso de programas de monitoreo.

Alcance: Todas las áreas con tecnología Informática del colegio, así como todos los usuarios autorizados a usar las TIC.

Desarrollo:

- El jefe de informática con previa coordinación y aprobación de la Gerencia, autorizará al Administrador de la red a utilizar herramientas de comprobación y monitoreo.
- El Administrador de la red utilizará herramientas de comprobación y monitoreo para detectar fallas en el sistema implantado en la institución.
- El Administrador de la red implementara medidas para eliminar las vulnerabilidades detectadas por los programas de monitoreo y comprobación.
- Los programas de monitoreo serán usados en función del mejoramiento continuo de la red de datos.

Procedimiento # 11 Introducción de Aplicaciones Informáticas.

Objetivo: Que las aplicaciones informáticas estén evaluadas y cumplan los requisitos de seguridad informática.

Alcance: A todas las aplicaciones informáticas de uso colectivo o uso local.

Desarrollo:

- Las aplicaciones instaladas en las computadoras, serán evaluadas por el jefe de informática y aprobadas por la Gerencia.
- Estas serán instaladas por el área de informática únicamente o por un personal que determine la Gerencia.
- No está permitida la descarga de aplicaciones por estudiantes.
- Las aplicaciones instaladas en la institución, tendrán dos fines:
  - Educativo
  - Informático
- Las aplicaciones que no cumplan objetivo o estén desactualizadas, serán eliminadas por las versiones posteriores.
- El Encargado de la Actividad Informática son los encargados de la instalación de los productos de software.
- Los Jefes de Departamentos decidirán a que puestos de trabajo se instalaran los productos de software y que usuarios utilizarán el mismo, si no tienen autorización proceder a solicitar la misma.
- El Encargado de la Actividad Informática realizará pruebas de los productos de software instalado en el puesto de trabajo.
- El Administrador de la Red o el Encargado de la Actividad Informática son los encargados de la instalación de las aplicaciones de uso colectivo en los servidores de la red de nuestra entidad.
- El Administrador de la Red asignará los derechos y permisos asignados a los usuarios que van a utilizar la aplicación por parte de los Jefes de las Áreas.

Procedimiento # 12 Compartir Carpetas en la Red.

Objetivo: Establecer el procedimiento para compartir carpetas en la red de la institución.

Alcance: A todas las tecnologías informáticas del colegio.

Desarrollo:

- El jefe de cada área decidirá la información a compartir en su departamento.
- La información compartida solo será con fines de trabajo.
- Se podrá compartir a través de la red normalmente o en los sistemas que establezca el área de informática para ello.
- Los estudiantes compartirán información solo a través de los sistemas que establezca el área informática.
- Las carpetas se compartirán con accesos restringidos según clasificación de grupos.
- Eliminar cuando corresponda los accesos a carpetas compartidas.

Procedimiento # 13 Administración del Controlador de Dominio.

Objetivo: Establecer políticas de seguridad para el Dominio.

Alcance: Todos los usuarios, ordenadores y notebook de la red de datos.

Desarrollo: Para la configuración del controlador de dominio se utilizarán los siguientes sistemas y servicios:

- Windows server (actualizar versión según necesidad del colegio).
- Windows pro en estaciones de trabajo.
- Netsupport
- Configurar servidor DNS
- Configuración de Active Directory.
- Servidor DHCP en firewall meraki

- El Administrador de la Red es el encargado de configurar y aplicar las políticas de seguridad para el dominio, se ejecutará como base la siguiente configuración en el servidor de Controlador de Dominio:

  Políticas

  - Guardar en el histórico de las contraseñas: 6 contraseñas recordadas.
  - La edad máxima de la cuenta de 180 días.
  - La edad mínima de la cuenta de 30 días.
  - Longitud mínima de la contraseña de 8 caracteres.
  - Habilitar que las contraseñas requieran nivel de complejidad.
  - Duración de la cuenta bloqueada de 30 minutos.
  - Bloquear a 3 intentos inválidos.
  - Desbloquear la cuenta tras 30 minutos.
  - Auditar el inicio de sesión de las cuentas.
  - Auditar el manejo de las cuentas.
  - Auditar el acceso a los servicios de directorios.
  - Auditar el acceso a los objetos.
  - Auditar el cambio de política.
  - Auditar el uso de privilegios.
  - Auditar los eventos del sistema.
  - Deshabilitar la cuenta de invitado.
  - Renombrar la cuenta del administrador.
  - Otras que resulten necesarias para el control y seguridad de la red de datos.

- El jefe de Informática velará por la aplicación de este procedimiento.

Procedimiento # 14 Administración del Firewall

1. Crear vlan para segmentación de las diferentes redes
2. Distribuir equitativamente el ancho de banda.
3. Configurar DHCP para distribución de IP internas
4. Implementar políticas y reglas generales
5. Crear y administrar usuarios super admin.
6. Monitorear comportamiento y uso de la red de datos.
7. Restringir accesos a sitios vulnerables o con contenidos violentos y sexuales.
8. Actualizar las licencias de operatividad.
9. Establecer los accesos VPN según corresponda.
10. Otras configuraciones necesarias para mantener y reforzar la seguridad de la red de datos.

Procedimiento # 15 Conservación de las Contraseñas de Administración.

Objetivo: Conservar las contraseñas de administración de computadoras, aplicaciones o software.

Alcance: Todas las tecnologías informáticas, aplicaciones o software del colegio.

Desarrollo:

- El Administrador de la Red es el encargado de crear el usuario ADMIN para la administración de la red para casos de contingencia, este usuario tiene que ser diferente al que usa el administrador de la red.
- Las contraseñas de administración sólo serán de conocimiento y uso exclusivo del Administrador de la Red, el jefe del área y la Gerencia.
- Las contraseñas se actualizarán o cambiarán por solicitud del jefe de informática y cada vez que la Gerencia determine.
- Todas las contraseñas de administración de dominio, aplicaciones y del hosting, se mantendrán impresas y actualizadas bajo el mando de la Gerencia del colegio.

Procedimiento # 16 Normativa de seguridad de la información y acceso a sistemas

La normativa de las Tecnologías de la informática y las comunicaciones (TICs) y el uso responsable de las mismas, busca establecer las medidas de seguridad y obligaciones del trabajador en el uso de los bienes y servicios informáticos que provee la institución a los trabajadores como herramienta para el cumplimiento de sus funciones.

Delimitaciones Generales

Las infracciones a las normativas del departamento de Informática y Tecnología constituirán falta grave, para todos los fines previstos en la legislación laboral vigente.

De la Seguridad de la Información y Acceso a Sistemas

Es responsabilidad exclusiva de cada trabajador:

- **a)** Cumplir con las políticas, procedimientos y normas de seguridad que la Institución defina y difunda respecto de la información y sus respectivos flujos.
- **b)** Mantener absoluta confidencialidad sobre la información a la que tenga acceso y que se estime sea importante para los fines de la Institución.
- **c)** Proteger y resguardar toda la información de la Institución que disponga o administre, sea este fruto de su trabajo o que le haya sido remitida, sean estos reportes, informes, datos, proyecciones, estrategias u otros, así como de la información propia del área específica donde se desempeña, respecto de las cuales haya tomado conocimiento producto del ejercicio de sus labores.
- **d)** Hacer un uso diligente de sus claves de acceso, así como mantenerlas en secreto y no comunicarlas a terceros.
    - Cambiar periódicamente sus contraseñas, sin ser obvias, triviales o predecibles.
    - Solicitar la eliminación de aquellas cuentas o accesos que ya no requiera por cambios de funciones.

Está prohibido al trabajador:

- **a)** Intentar entrar a sistemas o servidores a los cuales no está autorizado, o que de acuerdo con sus funciones no les corresponda, sean estos locales de redes externas.
- **b)** Intentar infringir la seguridad de los sistemas y de la red local, o de cualquiera otra red accesible, desde los equipos de la red de la Institución.
- **c)** Intentar acceder a otras cuentas de sistemas, aplicaciones o cuentas de correo electrónico para las que no esté expresamente autorizado.

Procedimiento # 17 Normativa de la instalación, configuración, uso de software, hardware y servicio de soporte a computadores y notebooks…Normativa de seguridad de la información y acceso a sistemas

Los usuarios de software, programas y aplicaciones en los computadores de Saint Patrick School deberán tener en cuenta que los siguientes actos representan una clara violación a la política de uso informático de la Institución, consecuentemente se encuentra terminantemente prohibido:

a) Copiar o Instalar software en violación a los términos de las licencias adquiridas por Saint Patrick School, o sin la licencia respectiva y autorizada por la Dirección de Informática y Tecnología.
b) Desinstalar programas, borrar archivos o cambiar configuraciones de los computadores de Saint Patrick School, sin autorización de la Dirección de Informática y Tecnología.
c) Reconfigurar el software de los computadores asignados al trabajo diario del personal.
d) Instalar y/o utilizar software para ver Televisión online, escuchar Radio vía internet o música online.
e) Instalar y/o utilizar software para descarga de información, como Torrent, Emule, Edonkey, Overnet, Kazza, Ares y genéricos o aplicaciones con vulnerabilidades de seguridad.

La instalación de software sólo debe ser realizada por personal de Soporte Técnico, o de la Dirección de Informática y Tecnología, de acuerdo con los procedimientos establecidos.

Del Uso de Equipamiento Computacional

Los usuarios de equipos computacionales, impresoras u otro equipamiento informático, de Fundación Saint Patrick School, deberán tener en cuenta que los siguientes actos representan una clara violación a la política de uso informático, consecuentemente les está prohibido:

a) Destruir recursos de computación.
b) Usar sin autorización o fuera de los horarios habilitados los computadores y software.
c) Reubicar sin autorización de la Dirección de Informática y Tecnología o de

Soporte Técnico, los computadores o el equipamiento computacional instalado.

d) Operar los recursos de computación en forma que perjudique a los recursos informáticos, incluyendo las redes de computadores

e) Reconfigurar el hardware de los computadores o del equipamiento computacional asignado para las tareas diarias.

f) Utilizar los computadores para cometer delitos informáticos.

g) Utilizar indebidamente los recursos de computación con fines personales.

h) Utilizar los recursos con fines comerciales o recreativos (juegos, Chat o conversación electrónica en tiempo real, etc.).

Del Servicio de Soporte a Usuarios, Computadores y Notebooks

El servicio de soporte a usuarios, y soporte a computadores y notebooks de propiedad de la Institución, se podrá entregar en las siguientes formas:

a) De manera presencial o utilizando herramientas de control o acceso remoto a los equipos computacionales de los usuarios, cuando éstos lo soliciten, o bien, cuando se requiera hacer mantenimiento de reparación o preventivo de los equipos. Para esto, Soporte Técnico cuenta con herramientas que permiten entregar a los usuarios este servicio.

b) Soporte Técnico, dentro de sus funciones, debe realizar inventario de computadores de propiedad de la Institución y del software instalado en ellos, para lo cual podrá acceder a estos equipos utilizando software que permita recolectar toda la información del computador en lo referido a características físicas, técnicas y a los programas computacionales instalados.

c) Los servicios de mantenimiento general de computadores y/o cambio de equipo, tienen considerado un respaldo de toda la información contenidos en ellos, esto, como medida de poder reestablecer todos los datos en caso de algún problema que se presente en dicho procedimiento.

Procedimiento # 18 Normativa del uso de correo electrónico e internet

Del uso del correo electrónico

Es responsabilidad del usuario:

a) Administrar de forma eficiente y responsable su cuenta de correo, eliminando frecuentemente los mensajes que ya no sean útiles y que ocupen espacio adicional. Para garantizar esto último, y beneficiar a todos los colaboradores por igual, existe un límite de espacio para cada casilla de correo, considerando que los recursos son limitados y que el objetivo de Saint Patrick School es mantener un óptimo nivel en este servicio.

b) Que el contenido de los correos y archivos adjuntos a los mensajes, sean textos, documentos u otro formato, deberán siempre estar referidos a temas laborales y estar escritos en un lenguaje formal y adecuado a su contexto.

Está prohibido al usuario:

a) Remitir o reenviar mensajes no solicitados y, en particular, publicidad, comunicaciones con fines de venta directa o con cualquier otra clase de finalidad comercial, mensajes no solicitados dirigidos a una pluralidad de personas con independencia de su finalidad (spamming)

b) Utilizar el Servicio con la finalidad de almacenar, distribuir, transmitir o difundir mensajes cuyo contenido:

- Contravenga, menosprecie o atente contra los derechos fundamentales y libertades públicas reconocidas constitucionalmente, en los tratados internacionales y en el resto del ordenamiento jurídico;
- Induzca, incite o promueva actuaciones delictivas, denigratorias, difamatorias, infamantes, violentas o, en general, contrarias a la ley, a la moral y buenas costumbres generalmente aceptadas, o al orden público;
- Induzca, incite o promueva actuaciones, actitudes o ideas discriminatorias basadas en motivos de sexo, condición sexual, raza, color, nacionalidad, descendencia o ascendencia, creencia religiosa, opinión política, edad, estado civil, sindicación u origen social;
- Incorpore, ponga a disposición o permita acceder a productos, elementos, mensajes y/o servicios delictivos, violentos, pornográficos, degradantes o, en

general, contrarios a la ley, a la moral y buenas costumbres generalmente aceptadas o al orden público;

- Induzca o pueda inducir a un estado inaceptable de ansiedad o temor a un tercero, sea este parte de Saint Patrick School o no;
- Induzca o pueda inducir a involucrarse en prácticas peligrosas, de riesgo o nocivas para la salud física y mental;
- Sea falso, ambiguo, inexacto, exagerado o extemporáneo, de forma que puedan inducir a error sobre su objeto o sobre las intenciones o propósitos del comunicante;
- Se encuentre protegido por un derecho de propiedad intelectual o industrial perteneciente a terceros, sin que el trabajador haya obtenido previamente de su titular la autorización necesaria para llevar a cabo el uso que da o pretende dar;
- Contravenga los secretos empresariales de Fundación Saint Patrick School o de terceros;
- Sea contrario al derecho a honor, honra, a intimidad personal y familiar o propia imagen de una persona, sin importar si ésta es trabajadora o se encuentra vinculada a Saint Patrick School;
- Infrinja la normativa sobre secreto de las comunicaciones;
- Constituya publicidad ilícita, engañosa o desleal y, en general, constituya competencia desleal;
- Incorpore virus u otros elementos físicos o electrónicos que puedan dañar o impedir el normal funcionamiento de la red, del sistema computacional o de equipos informáticos (hardware y software) de terceros o que puedan dañar los documentos electrónicos y archivos almacenados en dichos equipos informáticos;
- Provoque por sus características (tales como formato, extensión, entre otras) dificultades en el normal funcionamiento del Servicio de correo electrónico institucional.

c) Enviar contenidos socialmente inaceptables y/o que vayan en abierta contravención de las leyes y normas vigentes en Chile;

d) Utilizar las listas de distribución a las que pueda tener acceso a través del Servicio para el envío de publicidad, de comunicaciones con fines de venta

directa o con cualquier otra clase de finalidad comercial, de mensajes no solicitados dirigidos a una pluralidad de personas con independencia de su finalidad, o de cualquier otro tipo de mensajes no solicitados e inesperados.

El Usuario se compromete, en general, a utilizar el Servicio de conformidad con la ley, el orden público, la moral y buenas costumbres.

Del Uso de Internet

Es parte de la política interna de la Institución otorgar acceso a Internet a los trabajadores que, en virtud de las funciones que desempeñan, deban hacer uso de dichos servicios informáticos, para lo cual el trabajador tendrá las siguientes condiciones y limitaciones:

Es responsabilidad exclusiva de cada usuario:

a) Utilizar el servicio de internet de forma correcta y diligente, en este sentido, debe abstenerse de emplearlo con fines o efectos ilícitos o lesivos de los derechos, garantías e intereses de terceros

b) Está prohibido al usuario:

c) Utilizar el servicio de internet como elemento recreacional, de diversión o pasatiempo.

d) Utilizar cualquier servicio de televisión y/o radio en línea a través de internet, debido al alto consumo de ancho de banda que esto representa.

e) Utilizar el servicio internet para dañar, inutilizar, sobrecargar:

- El servicio informático de la Institución.
- Los computadores (hardware y software) de otros usuarios de IP Chile o internet en general.
- Documentos, archivos y toda clase de contenidos almacenados en equipos informáticos (hacking).

f) Utilizar internet para descargar música, películas, y cualquier otro tipo de archivos con fines que no sean para las funciones que desempeñan.

La Institución se reserva el derecho de acceso o monitoreo a través de las redes informáticas de SAINT PATRICK SCHOOL, sin previo aviso, de cualquier uso de Internet o Intranet, incluyendo la revisión de archivos individuales (no privados) mantenidos por los usuarios en los equipos asignados por la institución.

Procedimiento # 19 Condiciones y obligaciones de uso del acceso remoto VPN

El usuario podrá recibir acceso a las conexiones remotas por medio del sistema VPN de SAINT PATRICK SCHOOL, por lo cual, el usuario declara estar en total conocimiento que:

a) Toda la información conservada en los equipos informáticos además de la que se encuentra en tránsito es de propiedad de SAINT PATRICK SCHOOL, por lo que podrá ser administrada y/o monitoreada por la Dirección de Informática y Tecnología de acuerdo con políticas de Seguridad establecidas.
b) Todo intento de ganar acceso a recursos no asignados a mi Usuario será considerado “intento de violación a la seguridad informática” por lo que SAINT PATRICK SCHOOL se reserva el derecho de tomar las acciones pertinentes al caso.
c) Las obligaciones contraídas en este acuerdo no prescribirán al finalizar la relación con Saint Patrick School

El usuario se compromete a:

a) No divulgar o utilizar la información disponible en los sistemas para fines contrarios a los intereses de SAINT PATRICK SCHOOL.
b) No revelar la contraseña de Usuario otorgada por SAINT PATRICK SCHOOL.
c) No permitir la utilización de la cuenta de Usuario y Contraseña por parte de terceros.
d) Solicitar la modificación de la contraseña de Usuario al sospechar que ésta haya sido descubierta.
e) Utilizar los sistemas de SAINT PATRICK SCHOOL únicamente para fines aprobados por éste.
f) Desconectarse de la estación de trabajo correspondiente, cada vez que finalice el uso del Sistema VPN.
g) El Servicio de VPN es de uso exclusivo del solicitante y no es transferible a terceros en ninguna circunstancia.
h) El Titular de la cuenta de VPN se hace responsable del uso que se haga de ésta. Por lo mismo, debe mantener bajo resguardo las claves de acceso al servicio.

Procedimiento # 20 Protección contra programas dañinos.

a) Instalación y Actualización de programas Antivirus.

Objetivo: Mantener los equipos informáticos libres de programas malignos.

Alcance: Todas las áreas con tecnología Informática.

Desarrollo:

- El administrador de redes, bajo la supervisión del encargado del área, es el encargado de la instalación de productos de software de antivirus.
- El Administrador de la Red habilitará los filtros y programas detectores en el servidor de mensajería.
- El Administrador de la Red habilitará en el servidor de antivirus que el este se actualice sistemática y automáticamente.
- El administrador de redes inhabilitará en todas las computadoras la auto ejecución de programas a través de soportes externos, puertos USB y lectores de discos.
- Los usuarios deben verificar sistemáticamente que su puesto de trabajo cuente con los productos de antivirus actualizados y de no ser así informar al Encargado de la Actividad informática.
- Los usuarios deben someter a revisión contra virus todo archivo que reciba por cualquier vía y realizar el chequeo del disco duro de su computadora no menos de una vez por semana.
- Los usuarios tienen la obligación de revisar mediante el antivirus, todos los pendrives, disco duro externo u otro medio portable que se conecte al computador para procesar información.

b) Pasos a seguir ante la detección de un virus informático.

Objetivo: Establecer los Pasos a seguir ante la detección de un Virus Informático.

Alcance: Todas las áreas con tecnología Informática.

Desarrollo:

Durante la explotación de los medios de automatización pueden presentarse los siguientes casos:

1. Al ejecutarse el programa detector de virus se descubre la existencia de áreas o ficheros contaminados en el disco duro.
2. Aún después de ejecutada la revisión con el programa detector de virus, al realizarse trabajos en la computadora se observa un comportamiento anormal (retardo en el procesamiento, perdidas de información, aparición de caracteres extraños en la pantalla, reseteo de la máquina sin causa aparente etc.) que haga sospechar la posible contaminación con virus desconocidos.
3. Al verificarse un soporte removible mediante el programa detector de virus se comprueba la existencia en el mismo de áreas o ficheros contaminados.

En el caso 1 y 2 debe procederse como sigue:

- Tomar nota del tipo de virus detectado, así como de los ficheros contaminados y otros datos reportados.
- Apagar la computadora, sin intentar realizar ningún tipo de acción para continuar la explotación.
- Comunicar al Encargado del área de informática sobre lo ocurrido, quién informará a la Gerencia y procederá a la descontaminación.
- En caso de que la versión instalada no descontamine por ser un virus que no esté incluido en la versión disponible se procederá a apagar la computadora y se le informará al Administrador de la Red y encargado del área para que gestione otra herramienta que pueda descontaminar el sistema.
- En el caso 3 para los soportes removibles, se procederá a informar al Encargado del área para descontaminar el medio.

Procedimiento # 21 Respaldo de la Información.

Objetivo: Establecer el procedimiento de respaldo que garanticen la continuidad de los procesos informáticos y la conservación de la información y los datos vitales que se procesan en la tecnología informática ante cualquier eventualidad o contingencia.

Alcance: Todas las áreas con tecnología Informática.

Desarrollo:

- **Los respaldos de los ordenadores se realizarán de la siguiente forma:**
  - Se utilizará una aplicación que cumpla los parámetros requeridos.
  - La frecuencia será en dependencia del nivel de seguridad de la información y se dividirá en diaria, semanal y mensual.
  - La ejecución se hará automática mediante la programación en la aplicación definida.
  - La información se replicará en los servidores, creando carpetas por cada área.
  - La periodicidad de retención del respaldo será por 5 años.
  - La principal fuente para el respaldo será el dispositivo NAS.

- **Los respaldos de los servidores se realizarán de la siguiente forma:**
  Respaldos Servidor SQL
  - Los respaldos se programarán automáticos con una frecuencia diaria.
  - La retención de respaldo de periodicidad será de 5 años.
  - Los únicos autorizados a modificar la programación del respaldo son los integrantes del área informática y contabilidad, autorizados previamente por la gerencia.

- **Respaldo de controlador de dominio:**
  - Se ejecutará mediante la configuración de discos duros RAID (disco espejo) o creación de imagen del Windows server.

Procedimiento # 22 Sitio Web e intranet del colegio.

Objetivo:

El sitio web: Se ocupa de difundir y promover el trabajo educativo, cultural, deportivo, pedagógico y profesional que desarrolla el colegio, además de dar a conocer las actividades diarias y características del centro.

La intranet: Se encarga de toda la información interna que circula y requiere el colegio.

Alcance: Todas las áreas del colegio (Intranet). Colegio y comunidad (Sitio web).

Desarrollo:

- Mantener actualizada todas las páginas que integran el sitio.
- Trabajar en el mejoramiento y modificación del diseño y formato, según las nuevas tecnologías y las necesidades del colegio.
- Reparar errores de la lógica cuando sea necesario.
- Garantizar el funcionamiento óptimo.
- Implementar sistemas de seguridad.

Procedimiento # 23 Topología y distribución de la Red de datos.

Objetivo: Establecer un flujo de información y organización de la red de datos, que contribuyan al buen funcionamiento de las tecnologías y por ende a un mayor aprovechamiento de los mismos.

Alcance: Todas las tecnologías del colegio.

Desarrollo: La topología de red a usar será la de **ESTRELLA**, teniendo en cuenta las características y necesidades del colegio.

Equipo	Puerto		Puerto	Equipo
Meraki	InternetPort		Internet 1	"@ internet Router
Meraki	1		Internet 2	"@ internet Router
Meraki	5		48 CORESW	CORESW
CORESW	47		48 ISLSW2-PS2	SWPS02
CORESW	46		48 ISLSW-RECT	SWRECTORIA
CORESW	45		48 ISLSW-PS01	SWPS01
CORESW	44		48 ISL.S-INF	SWS.INF
CORESW	43		48 ISL.S-INF	SWS.INF
SWS.INF	47		48 ISLSWGYM	SWGIMNASIO

Equipo	IP	Vlan
CORESW	192.168.254.1	254
SWPS02	192.168.254.2	254
SWRECTORIA	192.168.254.3	254
SWSP01	192.168.254.4	254
SWGIMNASIO	192.168.254.5	254
SWRESERVA	192.168.254.6	254
SWS.INF	192.168.254.7	254

Procedimiento # 24 Sistema de cámaras de vigilancia.

Objetivo: Velar por la integridad de nuestros alumnos en el proceso de sus actividades y mantener el colegio bajo vigilancia en todo momento.

Alcance: Todas las áreas del colegio.

Desarrollo: Se instalará una cámara en cada sala, oficina y en las áreas exteriores que lo requieran para cumplir con los objetivos trazados.

Composición del sistema de cámaras:

- DVR (1) 32 puertos IP192.168.92.2: Cámaras de las salas
- DVR (2) 16 puertos IP192.168.92.3: Cámaras exteriores y espacios comunes
- DVR (3) 32 puertos IP192.168.92.4: Cámaras exteriores y espacios comunes

Acciones:

- Se les aplicará mantenimiento preventivo en las vacaciones de verano.
- Los encargados de informática son los responsables de reparar, enviar a reparar o sustituir según corresponda con previa autorización de la gerencia.
- Mantener inventariado y apto para cumplir su función.


Planta de Laboratorio
Planta de Sala de Informática
SIMBOLOGIA
SE ELIMINA
SE CONSTRUYE
SE MANTIENE
MURO
Planta de Modificaciones Nivel 1
Planta de Modificaciones Nivel 2

Procedimiento # 25 Equipos de sonido.

Objetivo: Garantizar las actividades, clases y eventos culturales del colegio con equipos de sonido que aporten al desarrollo de este.

Alcance: Todas las actividades, clases y eventos.

Desarrollo: Se entregarán o prepararán según corresponda, los equipos de sonido que posee el colegio durante los procesos que requieran de estos.

Acciones:

- En eventos y actividades generales en el gimnasio, un técnico del área informática y un profesor de música se ocuparán de operar los equipos.
- En clases se entregará a los docentes los parlantes portátiles mediante un registro de control.
- Estos se almacenarán en local del gimnasio con acceso restringido.
- Mantener inventariado y apto para cumplir su función.
- Los encargados de informática son los responsables de reparar o enviar a reparar según corresponda con previa autorización de la gerencia.
- Se les aplicará mantenimiento preventivo en las vacaciones de verano.

Procedimiento # 26 Plataformas digitales.

Objetivo: Garantizar funcionamiento continuo y seguro con empresas que se dedican al rubro específico que se requiere.

Alcance: Todas las actividades, clases y eventos.

Desarrollo: El administrador de la plataforma creará los usuarios según el perfil del usuario, con los permisos correspondientes.

Acciones:

- Monitorear el uso correcto de las plataformas.
- Establecer y modificar los permisos según las necesidades de trabajo.
- Garantizar el funcionamiento continuo de los sistemas.
- Agregar, desactivar y eliminar usuarios según corresponda.
- Orientar y capacitar a la comunidad en el uso.
- Facilitar los enlaces de acceso.