COLEGIO DE ESTUDIOS CIENTÍFICOS Y TECNOLÓGICOS DEL ESTADO DE HIDALGO.
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (INFORMATICA).

POLÍTICAS DE SEGURIDAD EN LA INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN.

INTRODUCCIÓN

La seguridad en sistemas es una de las preocupaciones más importantes para cualquier organización que maneje información sensible. En este manual, se presentan las políticas de seguridad en sistemas para el área informática de servidores locales, con el objetivo de establecer un marco que garantice la confidencialidad, integridad y disponibilidad de la información. Es menester que en los servicios tecnológicos y de comunicación se asegure su correcto funcionamiento, evitar el uso inadecuado, así como tratar de minimizar y contener amenazas a la seguridad de la información.

OBJETIVO

La dirección de informática establece políticas de seguridad en correspondencia con los objetivos del Colegio, publicando y manteniendo estas en toda la organización, las cuales se comunicarán a todos los usuarios de manera apropiada, accesible y comprensible, con la finalidad de concientizar al personal del Colegio, sobre la importancia de la infraestructura informática, servicios de red y manejo de la información.

ALCANCE

Los Lineamientos del presente documento de seguridad informática del Colegio de Estudios Científicos y Tecnológicos del estado de Hidalgo, aplica para directivos, personal de apoyo y terceros no vinculados directamente al CECyTEH, pero que presten su servicio y utilicen tecnología de información, equipos propios del Colegio o arrendados y a los equipos de personas externas que sean conectados a la red de la Dirección General de CECyTEH.

La revisión, así como del objetivo de las Políticas de seguridad en la infraestructura de tecnologías de la información, debe realizarse con una periodicidad mínima de una vez al año, o cuando se originen cambios en la entidad que puedan afectar la operación de los servicios Tics, o durante las revisiones periódicas que desde la dirección se ejecutan para asegurar la continuidad del sistema.

JUSTIFICACIÓN

El aumento en el uso de tecnologías de la información puede posibilitar brechas o fisuras en aspectos de seguridad con respecto a su utilización, por ello se hace necesaria una gestión de la información desde una perspectiva tecnológica a tres niveles: aseguramiento y control sobre la infraestructura (nivel físico), los sistemas de información (nivel lógico) y las medidas organizacionales (factor humano) desde una perspectiva tecnológica.

Por lo antes mencionado, se centrará en el aseguramiento y control sobre la infraestructura la cual nos indicará el estado actual en que se encuentra la organización, por otra parte, las redes de datos son un factor fundamental siempre y cuando éstas estén disponibles constantemente, no presenten interrupciones y su rendimiento sea óptimo por lo que es necesario detectar inconsistencias y riesgos provocados por fallos en la red.

Por ello, es fundamental que el Colegio realice periódicamente y basado en una metodología identificar claramente los activos, las amenazas y las salvaguardas que poseen, para posteriormente diseñar estrategias que permitan el buen funcionamiento, la identificación de los puntos débiles de la organización y a partir de ellos establecer medidas que mitiguen los riesgos a que están expuestos los activos TI y su información.

Políticas de seguridad en equipos y cuentas.

Política de contraseñas de cuentas institucionales:

i. Todos los usuarios deben cambiar sus contraseñas cada 90 días.
ii. Las contraseñas deben ser de al menos 8 caracteres de longitud y contener caracteres alfanuméricos y símbolos.
iii. Las contraseñas no deben ser compartidas con otras personas o usuarios del Colegio.
iv. Los usuarios deben evitar el uso de contraseñas que sean fáciles de adivinar, como "123456" o "contraseña".
v. Los usuarios no deben utilizar contraseñas antiguas o previas.
vi. Los usuarios no deben utilizar la misma contraseña en múltiples cuentas.
vii. Los usuarios no deben almacenar contraseñas en archivos de texto, hojas de cálculo o cualquier otro lugar accesible para otros usuarios.
viii. Se debe requerir autenticación multifactorial para cuentas de alto riesgo, como cuentas de administrador o cuentas con acceso a información confidencial.
ix. Los usuarios deben recibir capacitación regular sobre la importancia de las contraseñas seguras y las mejores prácticas para crear y mantener contraseñas seguras.
x. Las cuentas deben bloquearse después de un número determinado de intentos fallidos de inicio de sesión.
xi. Los usuarios deben recibir notificación cuando su cuenta ha sido bloqueada.

Política de acceso a la información:

i. Restringir el acceso a los sistemas y datos a los usuarios no autorizados.
ii. Implementar un sistema de control de acceso que permita a los usuarios acceder solo a los recursos necesarios para su trabajo.
iii. Los usuarios deben estar obligados a cerrar la sesión o bloquear la pantalla de su computadora cuando se alejan de su escritorio.
iv. Los sistemas de información y los dispositivos de almacenamiento deben ser físicamente protegidos para evitar el acceso no autorizado.
v. Las cuentas de usuario deben ser creadas con niveles de acceso apropiados y se deben (ser) eliminar(das) cuando ya no sean necesarias.
vi. El acceso a los privilegios de administración debe limitarse a usuarios específicos.
vii. Los usuarios que tienen acceso a los privilegios de administración deben recibir una formación específica en seguridad y deben seguir un procedimiento de solicitud y aprobación para el acceso a los privilegios.

Política de respaldo y recuperación:

i. Realizar una evaluación de los sistemas de información para identificar los datos críticos y sensibles y los sistemas que deben ser respaldados.
ii. Implementar un plan de respaldo y recuperación para garantizar que los datos importantes se puedan recuperar en caso de un desastre.
iii. Los datos deben respaldarse regularmente y almacenarse en un lugar seguro y fuera del sitio.
iv. Se deben realizar pruebas periódicas para asegurarse de que el plan de respaldo y recuperación funcione correctamente.
v. Los medios de almacenamiento deben ser verificados y mantenidos de manera regular para garantizar que estén disponibles y listos para su uso en caso de una interrupción del servicio.

Política de seguridad de red:

i. Se implementarán medidas de seguridad de red para proteger los sistemas de ataques externos, como firewalls y sistemas de detección de intrusos.
ii. Se desactivarán los servicios y puertos de red innecesarios para minimizar la superficie de ataque.
iii. Se implementarán medidas de cifrado para proteger los datos en tránsito.

Política de seguridad física:

i. Se deben tomar medidas para proteger los sistemas y datos físicamente, como cerraduras en las puertas y en las salas de servidores.
ii. Los sistemas y equipos deben almacenarse en un lugar seguro y protegido contra daños y robos.
iii. Solo deben permitirse el acceso y la entrada a las personas autorizadas.

Política de actualización de software:

i. Se deben implementar medidas para garantizar que el software utilizado en los sistemas esté actualizado con los últimos parches de seguridad.
ii. Se deben establecer procedimientos para la gestión de actualizaciones de software, incluyendo la evaluación, la prueba y la implementación.

Política auditoría de tecnologías:

i. Se debe realizar una auditoría regular de los sistemas y la red para identificar posibles vulnerabilidades y brechas de seguridad.
ii. Las auditorías deben realizarse por personal externo e independiente.
iii. Se deben tomar medidas para abordar cualquier problema identificado en la auditoría.

Política de seguridad en personal de nuevo ingreso:

Notificación: La dirección de Administración a través del departamento de recursos humanos notificara a la dirección de informática, el nombre o los nombres del personal de nuevo ingreso, así como el número de empleado correspondiente, teniendo como finalidad proporcionarle lo que a continuación listamos:

i. Tomarse en la dirección de informática una fotografía con la finalidad de relacionar el nombre de la persona con su imagen correspondiente.
ii. Proporcionarle una credencial institucional del colegio a cada elemento que ingresa.

iii. Asignarle una cuenta de correo institucional con el dominio @cecyteh.edu.mx para que tenga sus notificaciones correspondientes y el uso de las aplicaciones de G-Suite de Google.
iv. Cuenta de acceso al sistema de información académica y administrativa según sus actividades a desarrollar.
v. Crearle y proporcionarle una cuenta de red y contraseña en el dominio del directorio activo una vez que le sea asignado equipo de cómputo.
vi. Notificarle al usuario que la información que se procese, se genere, modifique es solamente para uso y propiedad del colegio.
vii. Hacer énfasis al usuario que no debe usar cuentas de correo personal para los fines laborales.

Política de seguridad en personal que deja de prestar los servicios al colegio.

Notificación: La dirección de Administración a través del departamento de recursos humanos notificara a la dirección de informática, el nombre o los nombres de las personas que ya no forman parte del colegio, así como el número de empleado correspondiente, teniendo como finalidad de eliminar accesos y permisos que a continuación listamos:

i. Respaldar la información a solicitud de recursos humanos para que el usuario no elimine información propiedad del colegio.
ii. Entregar credencial del colegio.
iii. Validar que no tenga prestamos de equipos informáticos
iv. Validar que la información con la que se trabajó exista en el equipo que está entregando.
v. Inhabilitar inmediatamente la cuenta de correo asignada con la finalidad de que no haga mal uso de la información propiedad del colegio.
vi. Desactivar la cuenta de acceso al sistema de información académica y administrativa según sus actividades que desarrollo.
vii. Congelar la cuenta del directorio activo para que nadie use su perfil correspondiente en la computadora.

Políticas de seguridad en sistemas.

Acceso y autenticación

1.1. El acceso a los sistemas y datos deberá estar limitado a personal autorizado.
1.2. Cada usuario deberá contar con una cuenta única para acceder a los sistemas y se deberá implementar una política de contraseñas seguras que deberá ser renovada periódicamente.
1.3. Se deberá utilizar autenticación multifactorial para el acceso a los sistemas críticos.
1.4. Los usuarios deberán cerrar la sesión al salir de su equipo o al dejar de utilizar los sistemas.

Protección de datos

2.1. Se deberán implementar mecanismos de cifrado para proteger la información sensible en reposo y en tránsito.
2.2. Se deberá realizar copias de seguridad de la información de forma regular y se deberán almacenar en un lugar seguro y separado de los sistemas originales.

2.3. Se deberá establecer una política de retención de datos para garantizar que los datos se mantengan únicamente durante el tiempo necesario.

Seguridad física

3.1. Se deberán implementar controles de acceso físico para los equipos y salas de servidores.
3.2. Se deberá garantizar que los equipos estén ubicados en un lugar seguro y protegidos contra riesgos ambientales.
3.3. Los equipos deberán contar con sistemas de alimentación ininterrumpida (UPS) para proteger contra cortes de energía.

Monitoreo y registro

4.1. Se deberán implementar sistemas de monitoreo para detectar posibles amenazas de seguridad.
4.2. Se deberán establecer registros de actividad de los sistemas y se deberán analizar periódicamente para detectar posibles intrusiones.
4.3. Se deberán implementar sistemas de alerta temprana para notificar al personal responsable en caso de incidentes de seguridad.

Actualizaciones y parches

5.1. Se deberá contar con un plan de actualización y parcheo regular de los sistemas y aplicaciones para garantizar que se estén protegiendo contra las últimas amenazas de seguridad.
5.2. Se deberá realizar pruebas de vulnerabilidad periódicamente para identificar posibles puntos débiles en los sistemas.

Políticas de seguridad en el Site

Acceso:

- Se requiere que todas las personas que ingresen al centro de datos (SITE) se identifiquen y autentifiquen antes de ser admitidas. Esto mediante una bitácora de ingreso.
- Solo se permite el acceso al área del centro de datos solo a las personas que son necesarias para llevar a cabo las tareas autorizadas.
- El acceso de los visitantes al centro de datos debe ser supervisado por personal autorizado.
- Los usuarios deben ser conscientes de las políticas de seguridad y cumplirlas en todo momento.

Respaldos

- Se deberá identificar los datos críticos que deben ser respaldados. Esto incluye los datos de producción, como los archivos de la base de datos, los archivos de configuración del sistema, y otros datos importantes.
- Se establecerá los objetivos de recuperación, como el tiempo máximo de inactividad permitido y el tiempo máximo de pérdida de datos aceptable. Esto ayuda a determinar la frecuencia de los respaldos y el tipo de solución de respaldo a utilizar.
- Se recomienda la utilización de 3 discos, los cuales se deberán rotar durante un periodo de tiempo, con esto se evitará al máximo la perdida de información.
- Se diseñará un calendario de respaldos para garantizar que los datos críticos se respalden de manera regular y consistente, este incluirá la frecuencia, la hora y los tipos de respaldo a realizar.

- Se verificará regularmente los respaldos para asegurarse de que los datos críticos se hayan respaldado correctamente, la realización de pruebas de restauración y la documentación de las pruebas realizadas.
- Se mantendrá los respaldos en un lugar seguro y fuera del sitio.

Mantenimiento Correctivo y Preventivo

- Se realizará un cronograma de trabajo, con el fin de planificar cuidadosamente el proceso de mantenimiento, identificación de los equipos que se tienen en el lugar, la asignación de recursos para dicha actividad.
- Inspección visual de los equipos del centro de datos para identificar cualquier problema aparente, como la acumulación de polvo, cables sueltos o cualquier otra anomalía.
- El sistema de enfriamiento es crucial para mantener una temperatura adecuada en el centro de datos, por lo tanto, se verificará regularmente el sistema de enfriamiento (aire acondicionado, para garantizar su eficacia y detectar cualquier problema de manera temprana.
- Actualización regular del firmware y el software de los equipos, incluyendo los servidores, los sistemas de almacenamiento y otros dispositivos.
- Se documentará todo el trabajo de mantenimiento realizado en el centro de datos, incluyendo las inspecciones, limpiezas, reparaciones y actualizaciones.

Conclusiones

Las políticas de seguridad en la infraestructura de tecnologías de la información presentadas en este manual, deberán ser implementadas de forma rigurosa para garantizar la protección de la información sensible manejada por el área informática de servidores locales y a la infraestructura. Se deberá realizar una revisión periódica de estas políticas para asegurarse de que están actualizadas y adaptadas a las necesidades de la organización.

MARCO TEÓRICO

Activos: Recursos que forman parte de la organización como hardware, software, datos, infraestructura.

Amenaza: Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad de la información, los elementos de Información.

Ciclo PDCA: También conocido como Ciclo PHVA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales.).

Confidencialidad: es una de las propiedades de los activos de información que garantiza que solo personas autorizadas pueden acceder a esta.

Datos: Son todos aquellos conceptos, cifras, instrucciones que se tienen aisladas entre sí, sin seguir una organización o un orden específico.

Disponibilidad: característica de los activos que implica el acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requieran.

Hardware: parte tangible de un equipo de cómputo o dispositivo tecnológico, es decir, todos sus componentes físicos.

Información: conjunto de datos, añadidos, procesados y relacionados, de manera que pueden dar pauta a la correcta toma de decisiones según el fin previsto.

Integridad: cualidad de los activos de información donde se asegura que la información y sus métodos de proceso se mantengan exactos y completos.

Mantenimiento Correctivo: proceso mediante el cual se realizan las correcciones de las averías o fallas, de un equipo de cómputo, cuando éstas se presentan.

Mantenimiento Preventivo: es el conjunto de actividades que se desarrollan con el objeto de proteger los equipos de posibles fallas, utilizando métodos de limpieza física y también métodos basados en el uso de software.

Política de Seguridad: consiste en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Seguridad de la información: es todo el conjunto de técnicas y acciones que se implementan para controlar y mantener la privacidad de la información y datos de una institución; y asegurarnos que esa información no salga del sistema de la empresa y caigan en las manos equivocadas.

Sistema de Gestión de Seguridad de la Información: proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.

Software: son todos los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.

Trazabilidad: propiedad de los activos de información que permite asegurar que en todo momento se podrá determinar quién realizó cierta actividad y en qué momento lo hizo.

Vulnerabilidad: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Sistema de Gestión de Seguridad de la Información: proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.

Software: son todos los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador.

Trazabilidad: propiedad de los activos de información que permite asegurar que en todo momento se podrá determinar quién realizó cierta actividad y en qué momento lo hizo.

Vulnerabilidad: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

	Elaboró:	Autorizó:
Puesto	**Director de Informática**	**Director General**
Fecha		
Nombre y firma	**Aldo Serafín Pedraza Montiel**	**Agustín Rowe Córdova**