Plan de Seguridad y confianza digital

Plan CoDiCe de centro

CONTROL DE MODIFICACIONES			
EDICIÓN	FECHA	MODIFICACIONES RESPECTO A LA REVISIÓN ANTERIOR	PROPIETARIO
Ed. 0	Enero 2024	Creación del documento.	Rosalinda Cabria Bahamonde
Ed.1	Febrero 2024	Versión resumida	Rosalinda Cabria Bahamonde

Contenido

OBJETIVOS

Objetivo general

- Establecer una estrategia para proteger la información digital generada en el centro , para reducir riesgos y promover el uso seguro de dispositivos e internet
- La correcta aplicación del plan , evita riesgos y peligros y contribuye a la protección de datos del centro y miembros de la comunidad educativa

Objetivos específicos

- Proteger Infraestructuras TIC
- Proteger información en base a la normativa de protección de datos
- Evitar pérdidas de información

ALCANCE

Este plan debe ser aplicado por todos los miembros de la comunidad educativa que tengan acceso a las infraestructuras TIC y/o información del centro

Para elaborar este Plan se ha tenido en cuenta:

- Tipo de usuarios
- Tipo de infraestructuras
- Control de acceso
- Conectividad de dispositivos del centro
- Posibles riesgos en los dispositivos y conectividad
- Prevención de riesgos
- Actuaciones en caso de incidencias
- Gestión de copias de seguridad
- Registro de incidencias que se hayan producido en cursos anteriores
- Auditorías internas

ASIGNACIÓN DE ESPACIOS Y EQUIPOS TIC. CONTROL DE ACCESOS

- Al final del curso escolar cada profesor, en función del módulo que imparte, y previsión de actividades que impliquen uso de TIC, solicita un determinado número de horas semanales para disponer de equipos informáticos para el curso siguiente.
- Antes del inicio de curso, la jefatura de estudios asigna a cada grupo espacios y equipos, a partir de las necesidades que comunicó cada docente
- Se asigna un laboratorio/armario de portátiles y un horario fijo para todo el curso, permitiendo que todos los alumnos del centro puedan utilizar los equipos.
- En el caso de que necesite alguna hora más de modo puntual, puede reservarla con antelación en función de los espacios disponibles , solicitándolo al jefe de estudios o . reservar los equipos portátiles en un documento compartido en drive por cada departamento
- Los accesos y responsabilidades se detalla en otro documento más amplio a disposición del profesorado del centro

ESTRUCTURA ORGANIZATIVA DE SEGURIDAD Y RESPONSABILIDAD SOBRE LOS DATOS PERSONALES Y DOCUMENTOS INSTITUCIONALES Y RECURSOS DE ENSEÑANZA APRENDIZAJE

Estructura organizativa de seguridad y responsabilidad sobre la seguridad, datos personales, documentos institucionales y recursos de aprendizaje y enseñanza.

Existe un nivel de protección de datos elevado, que garantiza la **confidencialidad de datos** coordinado por secretaría del centro, y una empresa externa

Es responsabilidad de todo el profesorado y comunidad educativa cumplir con la normativa existente al respecto

Descripción del contexto de almacenamiento y custodia de datos académicos, didácticos y documentales.

- Existe una política de copias de seguridad de la información de esa unidad de red ubicada físicamente en el servidor.
- Por seguridad, se eliminan los datos alojados en cada equipo. Para ello, al principio y a final de cada curso académico una empresa externa se encarga de hacer un formateo de los equipos y reconfiguración de todo el sistema.

ESTRATEGIAS DE SEGURIDAD DE SERVICIOS Y REDES

Los datos de información técnica relativa a protección frente a intrusiones no deseadas, control de acceso al wifi, contenidos de internet y actividad se detalla en otra versión más amplia de[RC1] **este documento**

Profesorado:

- El profesor debe apagar la pizarra digital, y cerrar sesión al salir del aula.
- El profesorado accede con cuenta de profesor
- Cada profesor es responsable de sus dispositivos de uso personal
- Las memorias USB o dispositivos de almacenamiento extraíbles con datos sensibles de alumnos deben estar cifradas
- El profesor debe comprobar que cada alumno/a usa el equipo asignado y al terminar lo cierra y deja en perfecto estado
- El centro no se hace responsable de los dispositivos personales de profesores

Alumnos

- Deben cerrar sesión en todas sus cuentas y apagar el ordenador al término de la clase cuando use ordenadores, equipos portátiles y dispositivos móviles
- No está permitido el acceso de usuario de los alumnos en ningún equipo que esté conectado a pizarra digital, y tampoco pueden usar los ordenadores del laboratorio de informática ni biblioteca sin la supervisión de un profesor.
- Los alumnos no pueden acceder al servidor donde se almacena la documentación generada por el profesorado, documentos de centro etc

- Deben comunicar cualquier incidencia al profesor de modo inmediato
- Los alumnos acceden con la cuenta de su curso
- El centro no se hace responsable de los dispositivos personales de alumnos

Redes sociales: Presencia del centro en internet e identidad digital institucional

Recurso	Acceso	Uso	Responsabilidades
Web de centro Construida sobre Wordpress posicionamiento mediante: palabras clave, entradas de actividades, SEO, links a otras webs, intentando captar links a la nuestra, SEM a través de la publicación de anuncios en google adwords. https://gregoriofer.com/	Solo el responsable de la web puede hacer publicaciones y modificaciones con la aprobación del equipo directivo	Información del centro (notas de identidad, Organización Instalaciones, Documentos públicos etc) Oferta educativa Blogs de ciclos Secretaría (documentación, becas, etc) Calidad(misión, visión y valores, encuestas, Premios,proyectos, buzón,,) Noticias certificaciones	Cada profesor envía al responsable lo que quiera publicar en la web previa autorización del equipo directivo
Blog de cada ciclo Enlazadas a la web de centro	A cada blog solo tiene acceso el coordinador de cada departamento. A criterio del coordinador y por	Información sobre el ciclo, difusión de actividades de los alumnos, información de interés	Los profesores que tienen acceso a cada blog. Deben cumplir la ley de protección de datos y respetar los derechos de

	acuerdo con su equipo docente, también puede acceder profesores del departamento		uso
Revista digital Colgada en la web de centro https://gregoriofer.com/revista-gregorio-fernandez/	Coordinador de la revista. Los alumnos envían sus aportaciones al tutor de cada grupo, y este al coordinador de la revista También pueden participar familias y profesores	Difusión de actividades realizadas por los alumnos, Contribuye al plan de lectura a través de contribuciones de los alumnos en forma de relatos	Las publicaciones de deben cumplir la ley de protección de datos y respetar los derechos de uso
Redes sociales: Facebook X Instagram Canal YouTube	Profesorado	Educativa y divulgativa	Se debe aplicar el plan de comunicación La profesora responsable de redes, revisa periódicamente las publicaciones y elimina los comentarios inapropiados
Bolsa de empleo https://bolsadeempleo.gregoriofer.com/	Dpto de FOL Alumnos del centro con clave	Empleabilidad del alumno y motivación	Se publican ofertas de empleo clasificadas por ciclo formativo

NORMAS DE USO DE INFRAESTRUCTURAS TIC DEL CENTRO

1. Tienen derecho a acceder al uso de los equipos de informática de laboratorio y armarios portátiles, el profesorado y alumnado que acrediten su calidad de alumno/a del centro.
2. No está permitido el acceso de usuario de los alumnos/as en ningún equipo que esté conectado a pizarra digital, y tampoco pueden usar los ordenadores del laboratorio de informática sin la supervisión/permiso de un profesor/a
3. El uso de los recursos informáticos es sola y exclusivamente para fines académicos, quedando prohibido el uso del ordenador para otros fines (juegos, chats, realizar descargas no autorizadas, borrar o copiar datos de carpetas compartidas por profesores, etc.).
4. No se permite el acceso a sitios web que atenten contra la integridad, la moral y las buenas costumbres.
5. No se permite manipular físicamente ningún equipo. Ej.: cambiar ratón, monitor o teclado de sitio, cables de red, etc.
6. Los alumnos/as utilizarán únicamente los ordenadores asignados por el profesorado.
7. Se deberán apagar o suspender las sesiones iniciadas entre clase y clase, además de los monitores, especialmente en el recreo.
8. Los alumno/as no permanecerán en los laboratorios de informática durante los recreos.
9. En los laboratorios de informática o mientras se usan portátiles, está prohibido consumir cualquier tipo de alimentos o bebida.
10. Si por algún motivo un alumno/a recibe algún tipo de privilegio sobre los recursos de informáticos no podrá hacer uso indebido de ello.
11. El alumno/a se compromete a aceptar las normas de uso de los recursos informáticos del centro, incluida la red, con fines puramente educativas y de investigación, lo que excluye cualquier uso comercial así como prácticas desleales (hacking) o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información. En particular **quedan expresamente prohibidas las siguientes acciones:**

    - Tratar de causar daño a sistemas o equipos conectados a la red.
    - Diseminar "virus", y otros tipos de programas dañinos.
    - Ejecutar programas portables.

- Utilizar live CD's/live USB's.
- Congestionar intencionalmente enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.

12. Actuación ante incidencias de infraestructuras

- Se deberá comunicar al profesor responsable cualquier deficiencia o funcionamiento anómalo que se observe
- El profesorado comunicará la incidencia desde el formulario de mantenimiento de equipos informáticos

13. Incidencias por uso indebido

- El no cumplimiento de este reglamento implicará las sanciones correspondientes, de acuerdo a la falta cometida. Estas sanciones están recogidas en el Plan de Convivencia del Centro.
- Artículos del código penal aplicables para garantizar el buen uso de los recursos informáticos:

– Descubrimiento y revelación de secretos: Artículo 197 Código Penal
– Defraudación a través de equipo terminal de comunicaciones: Artículo 256 Código Penal Acceso indebido a sistemas informáticos: Artículo 174b Código Penal
– Sabotaje de sistemas informáticos: Artículo 175 Código Penal
– Acceso indebido a datos: Artículo 146b Código Penal
– Interceptación de datos: Artículo 146c Código Penal

14. Los usuarios de los equipos informáticos (laboratorios y/o armarios de portátiles) dan por entendidas y aceptadas todas las normas anteriores , comprometiéndose a respetarlas en todos sus puntos.

LAS NORMAS DE USO DE LOS LABORATORIOS DE ORDENADORES ESTÁN EXPUESTAS EN LOS TABLONES DE DICHOS LABORATORIOS.

ACTUACIONES DE FORMACIÓN Y CONCIENCIACIÓN DE USUARIOS DE LOS SERVICIOS DEL CENTRO

OBJETIVO

La finalidad de las acciones formativas dentro del plan de seguridad digital de centro son:

- Informar de las situaciones de riesgos más habituales cuando se navega por internet

- Formar sobre el uso seguro de internet
- Establecer unas buenas prácticas de uso de internet y dispositivos digitales para toda la comunidad educativa
- Promocionar el buen uso de las TIC a partir de la difusión de **Buenas prácticas en internet y uso de dispositivos digitales (** se detallan al final del documento)
- Lograr que todos los miembros de la comunidad educativa realicen un uso eficaz, seguro y responsable de las TIC

DESPLIEGUE

Desde el Plan de acción tutorial.

- Informar a los alumnos, de que el uso inadecuado de las TIC, puede ser un delito, y tener sanciones más o menos graves
- Informar de las sanciones que existen en el RRI y en el Plan de Convivencia del centro por uso indebido de las TIC
- Se dedicarán sesiones dentro de PAT para tratar el tema de la Seguridad digital. El material para las sesiones (videotutoriales), se encuentra en el curso TIC alumnos de moodle. Los posibles temas a tratar son:

    - Privacidad de los datos.

- Protección frente a virus, gusanos, troyanos, etc.
- Contraseñas seguras
- Cómo utilizar el correo y la mensajería instantánea de modo seguro.
- Redes sociales y problemas derivado de un uso inadecuado
- Huella digital
- Navegación segura
- Adicción a redes, internet, móvil…

- Solicitar los talleres y charlas de prevención de riesgos en internet que ofrece el Ayuntamiento dentro del plan de actividades municipales (cuando lo crea conveniente en función de las necesidades del grupo)
- Solicitar los talleres y charlas de INCIBE cuando lo crea conveniente en función de las necesidades del grupo

Desde el Plan de convivencia

Se aplicará la sanción que corresponda por uso indebido de las TIC, de acuerdo al reglamento de Régimen interno.

La comisión de convivencia revisará periódicamente las sanciones y se analizarán las incidencias.

Desde el departamento de Orientación

Dentro del plan de salud y bienestar, se ofrecerá formación al profesorado, y se facilitarán materiales de aplicación al aula, entre los que se puede tratar los problemas de adicciones a internet y dispositivos digitales

"Día de Internet Segura en el centro",

Este evento tiene lugar en febrero. Los alumnos del ciclo de SMR serán los encargados de planificar y organizar las distintas actividades para el resto de

alumnos del centro. El evento se difundirá en la página web y redes sociales del centro.

Las actividades que se realizarán podrán ser las siguientes:

- Campaña de concienciación del uso seguro de Internet, redes y dispositivos digitales. Dirigido a toda la comunidad educativa, mediante una breve presentación en las aulas, cortometraje elaborado por los alumnos, carteles, y actividades (kahoot de preguntas y respuestas, pasapalabra, etc).
- Se difundirán los materiales elaborados a través del blog del ciclo, redes sociales y web del centro, para facilitar el acceso a la información para toda la comunidad educativa https://gradomediosistemasmicroinformaticos.gregoriofer.com/
- Se tendrán en cuenta los contenidos e información de las web is4k
- Se fomentará las participación en actividades y talleres online, ofrecidas por INCIBE
- Cuando sea posible, se solicitará un Cibercooperante para que acuda al centro a dar una charla sobre alguno de los temas relacionados con el uso seguro y riesgos de internet

SEGUIMIENTO Y EVALUACIÓN

Al término de la jornada de internet segura, los alumnos y profesores realizarán un cuestionario/encuesta de autoevaluación para comprobar lo aprendido.

BUENAS PRÁCTICAS DE INTERNET Y USO DE DISPOSITIVOS DIGITALES

EQUIPOS

- Debes mantener actualizado el software de tu equipo
- Realiza copias de seguridad para poder recuperar datos
- El firewall de Windows debe estar activado.
- Desinstala o desactiva las app que no utilices.
- Si el equipo no es tuyo no dejes documentos
- Pon contraseña en todos tus dispositivos digitales y soportes de almacenamiento externos

NAVEGANDO POR INTERNET

- Pasa el antivirus periódicamente y mantenlo actualizado
- Mantén actualizado el navegador
- Es importante configurar la seguridad y privacidad de tu navegador.
- Evita los enlaces sospechosos y no escanees códigos QR si dudas de su fiabilidad
- Verifica la seguridad de sitios web antes de proporcionarles datos
- Comprueba que los sitios por los que navegas son fiables: visita sitios con HTTPS:// abre la información del candado en la barra de navegación. Comprueba que el certificado está vigente, y que estás en el sitio correcto
- Descarga las app solo de sitios oficiales y revisa los permisos.
- No ejecutes archivos sospechosos, solo si conoces su procedencia y son fiables
- No abras correos sospechosos
- Después de navegar elimina las cookies o configura el navegador para que se borren automáticamente. Otra opción es usar el modo privado o incógnito.
- Cierra sesión al terminar (en tu correo electrónico, plataformas educativas, etc que hayas entrado)

COMPRAS SEGURAS

- Comprueba que estas en un sitio seguro
- Evita redes públicas
- No guardes datos bancarios en la web o aplicaciones
- Desconfía de ofertas demasiado buena para ser ciertas
- No compartas información personal sensible
- Lee políticas de privacidad y devolución
- Evita comparar productos que aparecen en redes sociales

CONTRASEÑAS

- Usa contraseña con un mínimo de 8 caracteres.
- No uses palabras comunes o personales
- Usa palabras aleatorias difíciles de descifrar
- Incluye números, letras, mayúsculas, minúsculas y caracteres especiales
- Cambia las contraseñas , por lo menos cada tres meses
- No uses la misma contraseña para todo
- Nunca guardes las contraseñas en el navegador cuando te da la opción de recordar la contraseña.

PUBLICACIONES

- Contrasta la información que encuentres en internet, pues no todo lo que se pública es cierto
- Respeta los derechos de propiedad intelectual
- Aplica la Netiqueta

HUELLA DIGITAL

- Comprueba tu huella digital poniendo tu nombre y apellidos en el buscador (Configurar Google Alerts)
- Evita aparecer en muchos sitios de internet
- Comprueba tu configuración de privacidad de tus redes sociales
- Evita compartir demasiada información en las redes sociales
- Evita poner datos privados en redes WiFi públicas
- Elimina las cuentas antiguas que no uses
- Revisa tu uso de dispositivos móviles
- Piensa antes de hacer una publicación
- Actúa rápido después de una filtración de datos: cambia todas las contraseñas, avisa a tu banco etc
- Utiliza una VPN

SITIOS DE INTERÉS,

- INCIBE https://www.incibe.es/
- Is4k https://www.is4k.es/
- https://www.cyldigital.es/
- https://tucerticyl.es/formaci%C3%B3n-competencias-digitales
- https://empantallados.com/
- OSI https://www.osi.es
- Pantallas Amigas http://www.pantallasamigas.net/
- Plan de seguridad cfie, materiales http://cfievalladolid.centros.educa.jcyl.es/sitio/index.cgi?wid_seccion=55&wid_item=124
- Plan de seguridad y confianza en ámbito educativo. Materiales https://www.educa.jcyl.es/educacyl/cm/ciberacoso/gallery/Manuales/proteccion_antivirus.pdf
- SafeKids http://www.safekids.com/
- Safer Internet http://www.saferinternet.org/
- Seguridad en la Red http://www.seguridadenlared.org/
- http://www.fundacionaprenderamirar.org/
- https://gaptain.com/
- que es una VPN