5. PROTECCIÓN DE DATOS PERSONALES, PRIVACIDAD, SEGURIDAD Y BIENESTAR DIGITAL

0. Introducción

Esta es la úlltima competencia del *Área 1. Compromiso profesional* del Marco Digital Docente. Aquí abrazamos todo lo realizado anteriormente bajo el paraguas de la seguridad y el bienestar. Como docentes tenemos una gran responsabilidad con la cantidad de información a la que tenemos acceso, y es por eso que esta competencia es de vital importancia para entender la importancia de salvaguardar la información de propios y terceros (alumnado, familias..).

> Proteger los datos personales, las comunicaciones y el acceso a los dispositivos, dentro del ámbito educativo, para evitar los riesgos y amenazas que afecten a los derechos y garantías digitales de todos los miembros de la comunidad educativa contemplados en la normativa vigente. Utilizar de manera responsable, segura y saludable las tecnologías digitales para evitar riesgos laborales, personales y en el entorno y para garantizar el bienestar físico, psicológico y social del alumnado al utilizar las tecnologías digitales.

Esta competencia se concreta en la aplicación de las medidas y protocolos de seguridad en el centro, que deben desarrollar los establecidos por la legislación vigente. Aquí el plan digital del centros se presenta como un documento de centro donde alojar todos estos protocolos, ya que en él se deberá recoger el conjunto de medidas que garanticen el bienestar de la comunidad educativa.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

1. Información interesante sobre contraseñas.

> Una de las primeras barreras más importantes para evitar el uso fraudulento de nuestra identidad es tener una contraseña robusta y difícil de descifrar. Aquí te ponemos algunas características que una contraseña debería tener para responder a los criterios mínimos de seguridad.

1. CUALIDADES QUE DEBERÍA CUMPLIR UNA CONTRASEÑA:

- **Debemos asegurarnos que la contraseña tenga** una:
  - longitud mínima de doce caracteres,
  - que combine mayúsculas,
  - minúsculas,
  - números y
  - símbolos.
- **No debemos utilizar como claves:**
  - palabras sencillas en cualquier idioma,
  - nombres propios,
  - lugares,
  - combinaciones excesivamente cortas,
  - fechas de nacimiento,
  - etc.
- **Tampoco debemos usar claves formadas únicamente a partir de la concatenación de varios elementos**. Por ejemplo: “Juan1985” (nombre + fecha de nacimiento).

2. CUALIDADES QUE UNA CONTRASEÑA NO DEBERÍA TENER

Ejemplo de cómo deben ser las contraseñas

Oficina de seguridad del internauta.

https://www.osi.es/sites/default/files/quedeberiassaber/imagen-monografico-que-deberias-saber-contrasenas-ejemplos.png. *Imagen monográfico que deberías saber contraseñas ejemplos.*

Dentro de este artículo*https://www.osi.es/es/contrasenas* hacen el siguiente análisis de **cuanto tardaría un software** de combinación de caracteres en adivinar una contraseña **dependiendo de la combinación** que realizamos con los caracteres. Por un lado sería mezclando mayúsculas y minúsculas (todos los caracteres) y por otro solo minúsculas:

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

https://www.osi.es/es/contrasenas

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

2. Estrategias para una contraseña robusta.

Una vez visto que cualidades debe cumplir una contraseña para ser segura, vamos a ver diferentes estrategias para que además de ser segura también sea fácil de recordar y útil para nosotros. Es importante que cualquier **contraseña siga un proceso cognitivo lógico** para que si no recordamos exactamente los elementos de la contraseña, mediante el razonamiento lógico seamos capaces de deducirla.

> Es aconsejable utilizar **contraseñas diferentes para las diferentes plataformas** que utilicemos, ya que si se produce un grieta de seguridad en alguna de nuestras cuentas y quedamos descubiertos, estas credenciales servirían para poder entrar en el resto de cuentas.

En ocasiones, recordar todas las contraseñas que utilizamos (correo electrónico, redes sociales, mensajería instantánea, foros, etc.) puede resultar complicado. Para facilitar la tarea, podemos utilizar algunas sencillas reglas:

- **Cambiar las vocales por números**. Por ejemplo:
  - Mi familia es genial → M3 f1m3l31 2s g2n31l
- **Utilizar reglas mnemotécnicas**. Por ejemplo, elegir la primera letra de cada una de las palabras de una frase que sea fácil de recordar para nosotros:
  - Con 10 cañones por banda… → C10cpb…
- **Para hacer más sencillo el trabajo, podemos utilizar claves basadas en un mismo patrón, introduciendo ligeras variaciones para cada servicio**. Por ejemplo, tomando como base la contraseña anterior, añadir al final la última letra del servicio utilizado en mayúscula:
  - Facebook → C10cpb…K
  - Twitter → C10cpb…R
  - Gmail → C10cpb…L
- **Dependiendo del servicio y de su importancia podemos utilizar claves más robustas o menos, para facilitar su memorización.** Para los servicios más sensibles, siempre podemos utilizar un generador aleatorio de contraseñas. La mayoría de los gestores de contraseñas ofrecen esta funcionalidad.

> Otra razón para no utilizar la misma clave en diferentes servicios es el hecho de que **algunos** de ellos **no almacenan nuestra contraseña cifrada en sus servidores.** En

este caso, involuntariamente la estamos compartiendo con estos servicios, por lo que debemos poner una contraseña que no se parezca a ninguna de las otras que utilizamos. Una pista **para poder identificar estos servicios es comprobar si al darnos de alta o recuperar la contraseña nos indican cual era nuestra clave**, en lugar de proporcionarnos un enlace para cambiarla.

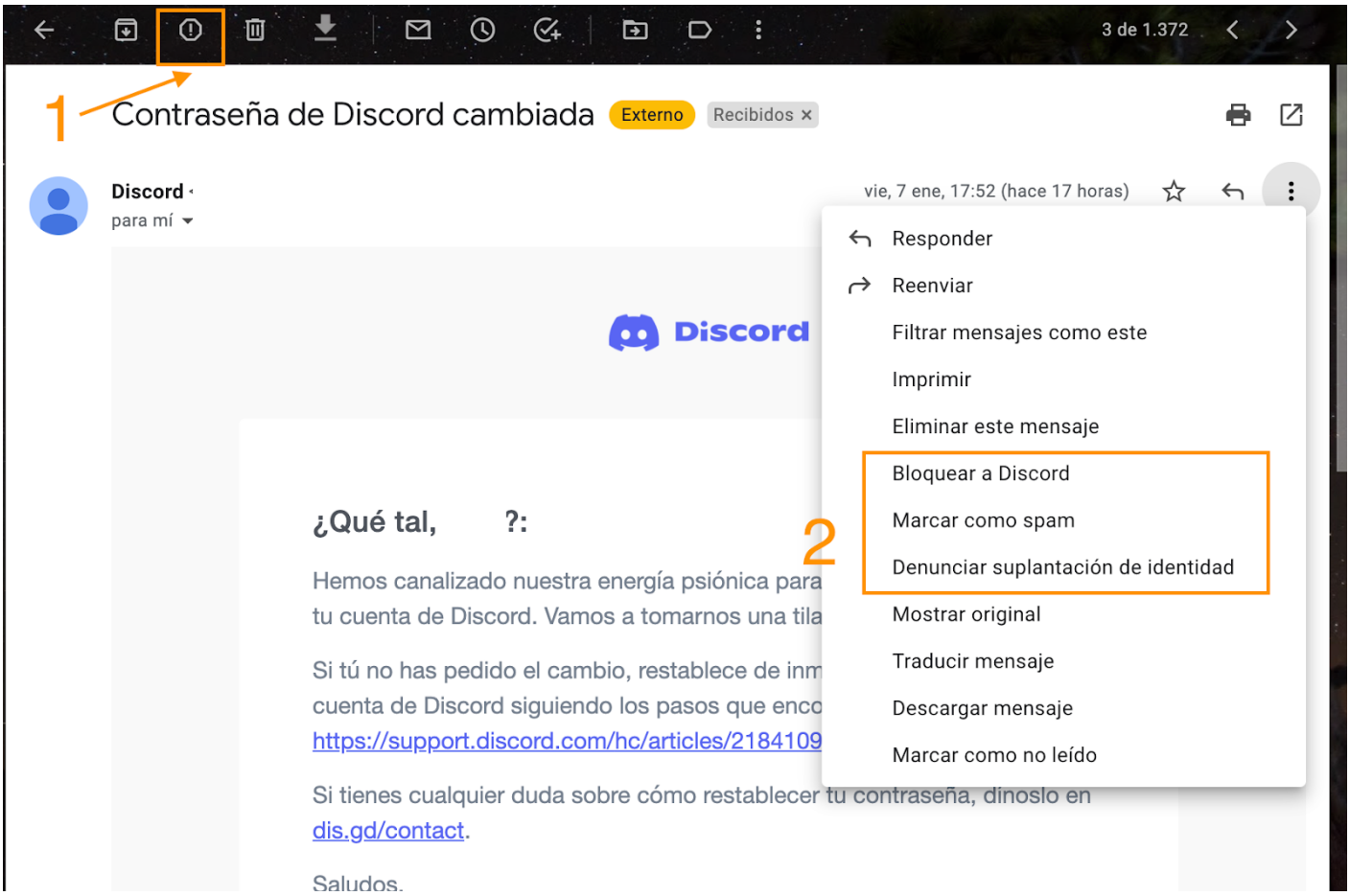
Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

3. Cómo gestionar el Spam

> El término ***spam*** **generalmente se refiere a las comunicaciones electrónicas no solicitadas** (típicamente mensajes de correo electrónico) o, en algunos casos, a las comunicaciones comerciales no solicitadas que se envían indiscriminadamente. **Algunos se refieren a este tipo de mensajes como *correo basura***. Si bien la actividad de spam toma mayormente la forma de mensajes de correo electrónico, el spam es una amenaza que evoluciona y s**e ha extendido a prácticamente todos los tipos de mensajes electrónicos, incluso a los mensajes SMS,** a las **publicacione**s en los medios sociales, a los si**stemas de mensajería instantánea y a los foros en línea .**

Si recibes un correo no deseado de forma regular, es mejor que lo marques como spam (correo no deseado), ganarás tiempo. En **Gmail** es muy sencillo. Podemos seleccionar varios correos no deseados y hacer clic en "**Marcar como spam**".

O, una vez en el correo cuyo remitente deseamos marcar como spam, hacemos clic en el menú de tres puntos, se desplegará un submenú y elegimos la opción de Marcar como spam. También podemos bloquear al remitente del mensaje o, si creemos que tiene suplantar una identidad o tiene fines maliciosos, podemos denunciarlo.



https://libros.catedu.es/uploads/images/gallery/2022-09/image-1663327505326.png

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

4. Phishing, qué es y cómo evitarlo

> El **phishing es una de las estafas con mayor trayectoria** y mejor conocidas de Internet. Es un tipo de fraude que se da en las telecomunicaciones y que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. La diferencia entre Spam y Phishing es clara: el Spam es correo basura, no es más que un montón de anuncios no deseados. **El phishing por otro lado, tiene como finalidad robar tus datos y utilizarlos contra ti.**

La **mayor parte del phishing puede dar como resultado el robo de identidades o de dinero, y también es una técnica eficaz para el espionaje industrial y el robo de datos**. “Algunos hackers llegan incluso a crear perfiles falsos en redes sociales, invierten un tiempo en desarrollar una relación con las posibles víctimas y esperan a que exista confianza para hacer saltar la trampa”.

Un ataque de phishing tiene 3 componentes:

1. El ataque **se realiza mediante comunicaciones electrónicas, como un correo electrónico, un SMS o una llamada de teléfono.**
2. El atacante **se hace pasar por una persona u organización** de confianza.
3. El **objetivo es obtener información personal confidencial**, como credenciales de inicio de sesión o números de tarjeta de crédito.

> Como a veces es difícil detectarlo, aquí te dejamos una serie de **características y trucos que pueden funcionar** para **detectar** un intento de **phishing:**

- Sé **precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales en el texto,** pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Si recibes **comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”,** es un indicio que te debe poner en alerta.
- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala seña**l. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.

- **Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta,** y que ésta corresponda con la URL del servicio legítimo.
- **Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas**. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la **ecuación: solicitud de datos bancarios + datos personales** = fraude.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

5. Uso y consumo de tecnologías digitales.

Este punto es muy importante, ya que **está directamente relacionado con nuestra salud.** El uso cada día más asiduo de las redes para la gestión prácticamente de cualquier cosa, hace que **a lo largo del día repitamos movimientos de forma continua** y mantengamos una **postura ergonómica relacionada con el dispositivo que usamos**. Esto significa que que **si el movimiento que repetimos es forzoso, a lo largo de los días desarrollemos una lesión** y acaba por condicionar nuestro estado de ánimo en el trabajo.

Es por ello que hay que **tener en cuenta los siguientes aspectos para tener** un uso sano de las tecnologías:

- **Aspecto postural**. Destacando la postura de la zona cervical y dorsal de la columna vertebral.
- **Aspecto visual**. En el que se destaca el uso prematuro de procedimientos de corrección de la graduación visual del menor por el uso de dispositivos digitales.
- **Aspecto mental**. Éste último es el que más preocupación produce en la sociedad actual, destacando:
  - El uso excesivo de dispositivos digitales, ya que el fin último es el consumo máximo de publicidad personalizada o encubierta por medio de influencers, la segmentación de perfiles para realizar acciones de marketing.
  - El ciberacoso o “bullying”, en el que se incluyen la difusión o recepción de bulos o fraudes que provocan desinformación o alarma social, el consumo o generación de discursos de odio, irrespetuosos o agresivos que pueden promover ideas extremistas, generando actitudes intolerantes o violentas y la pertenencia a comunidades que promueven conductas dañinas, trastornos alimenticios, autolesiones o consumo de drogas.

https://www.youtube.com/embed/cojLhNcBdBU

Youtube. Tu vida en las RRSS tiene público. Orange España

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

7. Ciberacoso.

UNICEF lo define como:

> Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.
>
> - **Difundir mentiras o publicar fotografías** o videos vergonzosos de alguien en las redes sociales.
> - **Enviar mensajes, imágenes o videos hirientes**, abusivos o amenazantes a través de plataformas de mensajería
> - **Hacerse pasar por otra persona** y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

Y por último, en el caso de que nuestro alumnado reciba el tan temido ciberacoso hay que enseñarles a gestionarlo:

- En un primer momento hay que **crear un clima de confianza con el menor** en el que entienda que se le escucha y se le apoya, evitando culpabilizar a nadie.
- Hay que **guardar evidencias** de la situación generada mediante capturas de pantalla de los mensajes, fotografías o vídeos.
- **Contactar con las Fuerzas y Cuerpos de Seguridad** en caso de reiteración, gravedad o ilegalidad del comportamiento.

IS4K de INCIBE. Ciberacoso escolar.

INCIBE es el Instituto Nacional de Ciberseguridad y tiene una web específica para el uso seguro en menores (IS4K). En ella se puede obtener más información sobre ciberacoso escolar en el siguiente enlace.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU