Seguridad y privacidad en internet

Pese a ser dos conceptos distintos, Seguridad y Privacidad van íntimamente relacionados. Conocer y aplicar normas de seguridad en internet, nos permitirá mantener a salvo nuestra privacidad y la de nuestra información.

Decálogo: 10 pasos hacia la ciberseguridad de Aragonesa de Servicios Telemáticos

Actualmente usamos diariamente las nuevas tecnologías tanto en casa como en el trabajo y, en este escenario, desde la **perspectiva de la seguridad de la información, hemos de tener mayor cuidado** pues, como empleados públicos que gestionamos información en primera persona somos el primer perímetro de seguridad de los datos que manejamos.

> De ahí, que sea clave nuestra implicación en la **gestión segura de la información**, desde la adopción de pautas de comportamiento seguro con las tecnologías hasta la integración de

medidas de mejora de la seguridad de la información con la que trabajamos.

A continuación, te presentamos **el Decálogo** que nos recomienda seguir el medio técnico del Gobierno de Aragón, Aragonesa de Servicios Telemáticos:

> “
>
> - **Puesto de trabajo.** Mantén la mesa “limpia” de papeles que contengan información sensible. Bloquea la sesión de tu equipo cuando abandones tu puesto. Es sencillo, pulsa a la vez [Tecla Windows + tecla L], tu equipo bloqueará la sesión automáticamente.
> - **Dispositivos.** Es mejor que no modifiques la configuración de tus dispositivos si no estás plenamente seguro de lo que quieres modificar. Es arriesgado conectar dispositivos USB no confiables y no está permitido instalar aplicaciones no autorizadas. En tus dispositivos móviles establece una clave de acceso y activa la opción de bloqueo automático.
> - **Uso de Equipos No Corporativos.** No manejes información corporativa en equipos de acceso público y, si accedes al correo del Gobierno de Aragón desde tu equipo personal, no descargues ficheros al equipo.
> - **Gestión de Credenciales.** No compartas tus credenciales de acceso (usuario y contraseña). Tus credenciales deben ser únicas e intransferibles. No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal porque pueden verse expuestas. No apuntes tus credenciales en lugares visibles.
> - **Correo Electrónico.** Fíjate en el emisor del correo y elimina todo correo sospechoso que recibas. Evita los correos en cadena, es decir el reenvío de correos que van dirigidos a un gran número de personas.
> - **Navegación.** Evita acceder a páginas webs no confiables y no pinches en enlaces (links) sospechosos. Es preferible escribir la dirección directamente en la barra del navegador y fijarse de que realmente accedes a donde quieres acceder.
> - **Viaja Seguro.** Procura no transportar información sensible en dispositivos extraíbles. Si lo haces, cifra la información. No manejes

información sensible en redes WIFI no confiables.

- **Protección de la información.** Realiza copias de seguridad de aquella información sensible que sólo esté alojada en tus dispositivos. Más vale un ‘por si acaso’ que un ‘no pensé’.
- **Fugas de Información.** No facilites información sensible si no estás seguro de quién es el receptor de la misma. Destruye la información sensible en formato papel (y si es con una destructora del papel, mejor). En todo caso, no la tires a la papelera.
- **Tú eres la Clave.** Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo, avisa al 4100.

A continuación, vamos a ver una serie de consejos para mantener a salvo nuestra privacidad:

Contraseñas seguras y robustas:

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

> 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

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.

Ayúdate de un gestor de contraseñas:

En la actualidad, manejamos distintas contraseñas para cada una de las actividades que realizamos: compras online, plataformas de streaming, correos electrónicos, gestiones bancarias.... todas y cada una han de ser distintas y cumplir unas condiciones muy particulares (mayúsculas, número de caracteres, con/sin símbolos...).

Por ello, los gestores de contraseñas se vuelven poderosos aliados ayudándonos a generar contraseñas tan seguras como aleatorias, y a tenerlas almacenadas para cuando nos son requeridas.

> Utiliza sólo gestores de contraseña en tus dispositivos personales y no en aquellos de uso público.

A continuación, encontrarás cinco gestores de contraseñas gratuitos y de código abierto:

- Keepass
- Bitwarden
- Passbolt
- Psono
- Teampass

Revision #7
Created 3 April 2023 09:29:25 by Alejandro Folch
Updated 8 June 2023 11:32:51 by Silvia Gómez Ferrer