Número 37 - Mayo 2024

# GESDEP

Revista

## Especial ciberseguridad

Asunto vital, también en tu club

## Delegado de protección de la infancia

La LOIPIVI en el deporte base

## Cambio de temporada en Gesdep

## ¡Adiós grupos de WhatsApp, adiós!

1234567890

# CIBERSEGURIDAD

## Mayor protección ante amenazas cada vez más reales y sofisticadas

Está ocurriendo en todos los ámbitos de la vida. La ciberdelincuencia es una industria que duplica el volumen del tráfico de armas y de drogas juntos; una auténtica barbaridad. Cada vez hay que estar más atentos ante la mayor frecuencia de intentos de estafa, así como por la sofisticación de los métodos empleados, que dificultan su identificación.

En Gesdep estamos decididos a plantar cara. En nuestra empresa tomamos ya las medidas más estrictas para evitar este tipo de situaciones, pero también queremos alertar a nuestros suscriptores, tanto clubes y entrenadores, para que dediquen un tiempo a analizar si se encuentran potencialmente en peligro, o con unas medidas de seguridad suficientes

Los ciberdelincuentes emplean una variedad de métodos para estafar a los usuarios. Aquí van los más conocidos hasta la fecha.

## MÉTODOS DE ACTUACIÓN DE LOS CIBERDELINCUENTES. DETALLE DE LAS AMENAZAS

**1. Phishing:**
Los estafadores envían correos electrónicos, mensajes de texto o crean sitios web falsos que parecen legítimos para engañar a los usuarios y que proporcionen información personal, como contraseñas, números de tarjetas de crédito o datos bancarios.

Ejemplo: Un correo que parece provenir de un banco solicitando la verificación de la cuenta.

**2. Spear phishing:**
Una forma más dirigida de phishing donde el ciberdelincuente investiga a su víctima para crear mensajes personalizados que aumentan la probabilidad de que el objetivo caiga en la trampa.

Ejemplo: Un correo personalizado dirigido a un empleado de una empresa, haciéndose pasar por un compañero de trabajo o un superior.

**3. Ransomware:**
Software malicioso que cifra los archivos del usuario y exige un rescate (generalmente en criptomonedas) para devolver el acceso a los datos. Hay que tener en cuenta que hay países en el que el pago de rescates es delito, como Estados Unidos, pero no en España. De todas formas, el pago no garantiza la recuperación de los datos. Incluso es posible que quien pide el dinero ya ni siquiera sea quien los robó, sino quien vendió la información obtenida en el robo.

Ejemplo: Un usuario descarga un archivo adjunto de un correo electrónico que contiene ransomware, lo que resulta en el cifrado de todos sus archivos.

**4. Ingeniería social:**
Tácticas que explotan la psicología humana para obtener acceso a información confidencial.

Ejemplo: Un estafador llama a un usuario fingiendo ser del servicio técnico de una empresa y le pide que proporcione su contraseña para "resolver un problema".

**5. Vishing (voice phishing):**
Estafas realizadas a través de llamadas telefónicas donde los estafadores se hacen pasar por entidades legítimas para obtener información personal o financiera.

Ejemplo: Una llamada telefónica que parece provenir del banco del usuario, solicitando detalles de la cuenta para verificar una actividad sospechosa.

**6. Smishing (SMS phishing):**
Similar al phishing, pero utilizando mensajes de texto para engañar a las víctimas y que hagan clic en enlaces maliciosos o proporcionen información personal.

Ejemplo: Un mensaje de texto que parece provenir de una empresa de mensajería, pidiendo al usuario que haga clic en un enlace para rastrear un paquete.

**7. Malware:**
Software malicioso que se instala en el dispositivo del usuario sin su conocimiento y puede robar información, dañar el sistema o tomar el control del dispositivo.

Ejemplo: Un usuario descarga un programa aparentemente legítimo que contiene spyware, el cual luego monitorea sus actividades y roba información confidencial.

**8. Fraude de comercio electrónico:**
Estafas que ocurren en plataformas de comercio electrónico, donde los estafadores venden productos falsos o inexistentes, o usan información de pago robada.

Ejemplo: Una oferta demasiado buena para ser verdad en un sitio web de ventas, donde el usuario paga por un artículo que nunca recibe.

**9. Estafas de suplantación de identidad (identity theft):**
Robo de información personal para hacerse pasar por la víctima y realizar transacciones fraudulentas.

Ejemplo: Usar la información personal robada para abrir cuentas bancarias o solicitar tarjetas de crédito en nombre de la víctima.

**10. Estafas de soporte técnico:**
Estafadores que se hacen pasar por técnicos de soporte para engañar a las víctimas y que paguen por servicios innecesarios o que instalen software malicioso.

Ejemplo: Una ventana emergente en el navegador que advierte de un virus y proporciona un número de teléfono para el "soporte técnico".

Estos métodos de estafa se basan en la explotación de la confianza, el desconocimiento y la falta de medidas de seguridad adecuadas por parte de las víctimas. La educación y la concienciación sobre estos métodos son cruciales para reducir la efectividad de las estafas.

# HABLEMOS AHORA DE PREVENCIÓN

Una vez vistas las amenazas, hablemos de soluciones. No se trata de actuar con miedo, pero es importante tener en cuenta que hasta las grandes empresas sufren ataques a pesar de destinar enormes recursos a evitar ese tipo de problemas. Cada vez es más importante crear hábitos seguros para evitar riesgos

Por tanto, cada entidad debe poner en marcha un plan de prevención con un mínimo coste que preserve su seguridad. Para ello transmitimos las 10 indicaciones básicas que recomienda el Instituto Nacional de Ciberseguridad, dependiente del Ministerio para la transformación digital y de la función pública

# MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

## Medidas básicas

**1. Contraseñas seguras:**
Crea contraseñas únicas y robustas para cada cuenta. Activa la autenticación multifactor (MFA, la doble autenticación con mensaje al móvil, por ejemplo) siempre que sea posible. No se las comuniques a nadie. Si utilizas un gestor o caja fuerte de contraseñas, estudia bien su reputación previa y su política de privacidad para asegurarte de que el gestor no tiene acceso a tus contraseñas, mantenlo actualizado y habilita la autenticación multifactor para el gestor.

**2. Actualizaciones de software:**
Mantén actualizado el sistema operativo, antivirus y aplicaciones. Activa las actualizaciones automáticas tanto en los equipos de sobremesa, portátiles como móviles. No instales aplicaciones desde fuentes no confiables.

**3. Copias de seguridad:**
Realiza copias de seguridad regulares de los datos importantes. Almacénalas en un lugar seguro y fuera del lugar de trabajo.

**4. Formación en seguridad:**
Capacita a tus colaboradores (por supuesto se incluye a los entrenadores) sobre las mejores prácticas de ciberseguridad. Conciéncialos sobre phishing, malware, suplantación de la identidad profunda mediante herramientas de Inteligencia Artificial generativa y otras amenazas.

**5. Protección de dispositivos móviles:**
Bloquea los dispositivos móviles con contraseñas o PIN y, si el dispositivo lo permite, preferentemente con la huella dactilar o reconocimiento facial. Instala también un antivirus y evita descargar aplicaciones de fuentes no confiables (las fuentes confiables son App Store (Apple) y Google Play (Android).

## Diagnóstico de riesgos

Evalúa los riesgos que está asumiendo tu entidad:

- ¿Qué información sensible manejas?
- ¿Quiénes tienen acceso a ella?
- ¿Qué medidas de seguridad existen actualmente?
- ¿Cuáles son las amenazas más probables?

Para ello te recomendamos una herramiento del INCIBE (Instituto Nacional de Ciberseguridad) para hacer un autodiagnóstico rápido de la ciberseguridad de tu club: “Análisis de riesgos en 5 minutos”

→ **ACCEDE AQUÍ** AL AUTODIAGNÓSTICO

# MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

## Política de contraseñas

Define quién tiene acceso a qué información y sistemas:

- Establece roles y permisos.
- Utiliza contraseñas seguras y el segundo factor de autenticación (MFA).

Aquí encontrarás unas checklists que el INCIBE recomienda en lo relativo al control del acceso a los distintos equipos y fuentes de información sensible de tu club: **ACCEDE AQUÍ**

## Antivirus / malware

Instala y actualiza software antivirus/antimalware:

- Realiza análisis periódicos
- Mantén el antivirus actualizado

Aquí tienes una entrada muy interesante del blog del INCIBE sobre recomendaciones con respecto a antivirus y antimalware: **ACCEDE AQUÍ**

## Actualizaciones de sistemas

- Sistema operativo
- Aplicaciones
- Controladores de hardware

Algunas pistas de cómo hacerlo: **ACCEDE AQUÍ**

## ¡Utilidades muy interesantes! (enlaces en letra negrita)

- **KeePassXC:** gestor seguro de contraseñas para que estén todas en un mismo sitio y con encriptación. Seguridad “casi” absoluta
- Microsoft y Google Authenticator para implementar el segundo factor de autentificación
- Las webs **osi.es** y **virustotal.com** verifican amenazas en programas, webs y documentos
- Herramienta **“Facilita”** para el cumplimiento de las políticas de Protección de datos (LOPD)
- **Have I Been Pwned (HIBP):** Comprueba si tu correo ha sido comprometido, filtrado o hackeado
- **Pentesting** o test de penetración: simula un ataque para detectar las debilidades de nuestro sistema
- Utilidad **“Clara”** del Centro Criptográfico Nacional, dependiente del CNI, creada para la detección y análisis de amenazas o “APTs” (Amenazas Persistentes Avanzadas)

# GESTIÓN DEL CAMBIO DE GRUPO DE DATOS

## CIERRA LA 23/24 Y DA COMIENZO A LA 24/25. PREPARA EL CAMBIO DE TEMPORADA

Estamos justo en ese momento en el que pronto comienza la nueva temporada, y toca gestionar el cierre de la actual y apertura de la que va a empezar. Hacer esto en Gesdep es muy sencillo, y nos irá creando año a año un histórico de información dentro del club muy importante para seguir la evolución de los jugadores/as y del propio club.

Se trata de un proceso importante. El no hacerlo generará una mezcla de datos de diferentes años que resultará en un caos importante. Hacerlo es muy conveniente y sencillo. Aquí t elo explicamos.

Para crear un grupo de datos nuevo (temporada) hay que seguir estos pasos:

- **Accede a 'Gestión' - 'Definir grupo de datos'**
- **Pulsa sobre 'Añadir'**
- **Introduce el nombre del nuevo grupo de datos, por ejemplo, 'Temporada 2024/2025'.** En el caso de ligas con torneos de apertura y clausura funcionaría exactamente igual
- **Haz click en 'Guardar'**


- **Principales:** Lo marcaremos como 'S' si queremos que sea este el grupo de datos por defecto cuando arrancamos la aplicación.

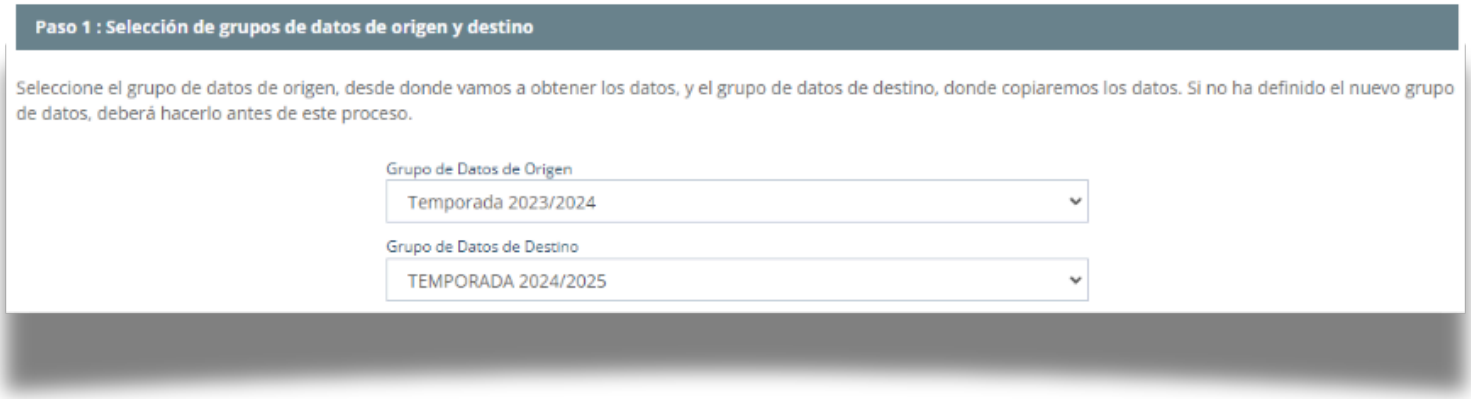
- **Activos:** Si ponemos 'N', dejaremos este grupo de datos inaccesible a los usuarios. Por ejemplo, mientras no nos interese que se acceda a la nueva temporada (los usuarios supervisores siempre podrán entrar).

- **Observaciones:** Cualquier comentario que se quiera incluir.

Una vez hecho esto hay que proceder al traspaso de la información de la temporada anterior a la actual.

Si creamos una temporada nueva y queremos incluir los jugadores de la temporada anterior sin tener que volver a darlos de alta, podemos hacerlo por medio de esta opción.

Al darle al botón “Traspasar entre grupos”, lo primero que nos pide es señalar cuál es el grupo de datos que contiene la información actual y a qué grupo de datos queremos enviarla:




Lo segundo que nos permite es traspasar los nombres de los equipos (sólo los nombres, no los jugadores) de un grupo de datos al otro:


Y por último, podemos traspasar la información de los jugadores. Aquí nos va a pedir el origen y destino de los jugadores, por ejemplo, los jugadores infantiles de la temporada anterior al equipo cadete de la actual. Esto traspasa todos los jugadores del equipo. Si hay algún jugador que sigue siendo infantil, vamos a la ficha y le cambiamos manualmente el equipo.

Cuando seleccionamos el equipo de origen, nos presenta solo los jugadores que aún no se han traspasado previamente y podamos seleccionar los jugadores a traspasar (por defecto están todos marcados). La lista incluye, aparte del nombre, la fecha de nacimiento, por si queremos seleccionar los que cumplen una cierta edad.

Y para acabar y que quede todo perfectamente claro, AQUÍ tienes un video explicativo del proceso.

# LEY DE PROTECCIÓN A LA INFANCIA

## y su implicación en el deporte base

### *¿EN QUÉ CONSISTE?*

La Ley Orgánica de Protección Integral a la Infancia y la Adolescencia frente a la Violencia (LOIPIVI) en España, aprobada en 2021, establece un marco integral de protección para menores, incluyendo medidas específicas para prevenir y abordar la violencia en todos los ámbitos donde los niños y adolescentes interactúan, incluyendo el deporte base.

### *PRINCIPALES COMPONENTES*

**Derechos de los menores:**

- Derecho a ser escuchados y a participar en decisiones que les afectan.
- Derecho a la protección frente a cualquier forma de violencia.

**Medidas de Prevención:**

- Programas de educación y sensibilización.
- Formación específica para profesionales que trabajan con menores.

**Detección y Actuación:**

- Protocolos obligatorios en educación, sanidad y servicios sociales.
- Figura del "Coordinador de Bienestar y Protección" en centros educativos.

**Protección y Atención a Víctimas:**

- Servicios especializados de atención integral.
- Medidas de protección urgente para menores en riesgo.

**Sistema Judicial:**

- Juzgados especializados en violencia contra menores.
- Procedimientos judiciales adaptados a menores.

**Medidas contra el acoso escolar y ciberacoso:**

- Protocolos para prevenir y actuar ante acoso escolar y ciberacoso.

**Control y Supervisión:**

- Autoridad Central de Protección a la Infancia y Adolescencia.
- Sistemas de seguimiento y evaluación.

## Su aplicación en el deporte base

El deporte base, que incluye todas las actividades deportivas practicadas por niños y adolescentes a nivel no profesional, es un área de especial atención en la LOIPIVI debido a su importancia en el desarrollo integral de los menores. Su aplicación en el deporte base implica varias medidas y acciones específicas. Estas son las recomendaciones:

**1.- Protección Integral:**

- Los clubes y entidades deportivas deben adoptar políticas y protocolos de protección infantil.
- Se requiere la figura del "Delegado de Protección" en las entidades deportivas, encargado de coordinar y supervisar las medidas de protección.

**2.- Formación y Sensibilización:**

- Formación obligatoria en protección infantil para entrenadores, monitores y otros profesionales del deporte.
- Programas de sensibilización para padres y jóvenes deportistas sobre los derechos de los menores y la prevención de la violencia.

**3.- Protocolos de Actuación:**

- Protocolos claros para la detección, notificación y actuación ante posibles casos de abuso, acoso o cualquier forma de violencia.
- Establecimiento de canales seguros y confidenciales para que los menores puedan denunciar situaciones de abuso o maltrato.

**4.- Entornos Seguros:**

- Creación de entornos seguros en las instalaciones deportivas, garantizando que se minimicen los riesgos de violencia y abuso.
- Políticas de acceso y supervisión en las instalaciones deportivas para proteger a los menores.

**5.- Participación y Escucha Activa:**

- Fomentar la participación de los menores en la toma de decisiones sobre su práctica deportiva.
- Establecimiento de mecanismos para escuchar y considerar las opiniones de los niños y adolescentes en asuntos que les afectan.

**6.- Colaboración Institucional:**

- Coordinación con organismos de protección infantil y autoridades locales para asegurar una respuesta integral y efectiva ante cualquier forma de violencia.
- Participación de las entidades deportivas en redes y programas de protección infantil.

# MENSAJERÍA GESDEP, TODO UN INVENTO

## ¿Quieres dejar de estar pendiente de los grupos de WhatsApp?

Hemos conseguido una mensajería instantánea creeos que diferente y bastante interesante. Tanto como para sugerirte que te decidas a dejar de utilizar grupos de WhatsApp o de cualquier otra app de mensajería.

Se trata de la comunicación directa,  unidireccional o bidireccional ¡tú eliges! entre el club y los jugadores, madres y padres.

El club selecciona a quien quiere hacer la comunicación. Puede hacerse a un solo jugador, a un equipo, o a un determinado número de jugadores aunque no pertenezcan al mismo equipo. En esto consiste la gran diferencia con los grupos de WhatsApp o cualquier otro sistema de mensajería; no es necesario crear grupos, sino que en cada momento se puede comunicar única y exclusivamente con las personas que quiero contactar

Además se puede ver quién ha leído y quién no los mensajes, enviar un aviso al correo electrónico además de al móvil, ¡y además decidor si permites que te respondan o no! ¿Qué más necesitas?