MANUAL DE BUENAS PRÁCTICAS EN CIBERSEGURIDAD

CEPA BERNAL DIAZ DEL CASTILLO

Protege tus conexiones

¿Sabes quién puede ver tu información si no te proteges bien?

1 Páginas web seguras

Asegúrate de que las páginas que visitas empiezan por https://. Esa "s" significa que tu conexión está cifrada y es más difícil que alguien la intercepte.

2 Contraseñas seguras

Usa contraseñas largas, mezclando letras, números y símbolos. Ej.: Gato3Azul!7 No repitas la misma contraseña en diferentes sitios.

3 Conexiones seguras

Si usas Wi-Fi en cafeterías o aeropuertos, activa una VPN (Red Privada Virtual) para cifrar tu conexión.

4 Dispositivos

Actualizar tu móvil o portátil no solo te da nuevas funciones, también corrige errores que los hackers pueden aprovechar.

5 Correos

Si recibes un correo que te pide datos o tiene enlaces raros, ¡no hagas clic! Puede ser phishing (intento de engaño para robarte información).

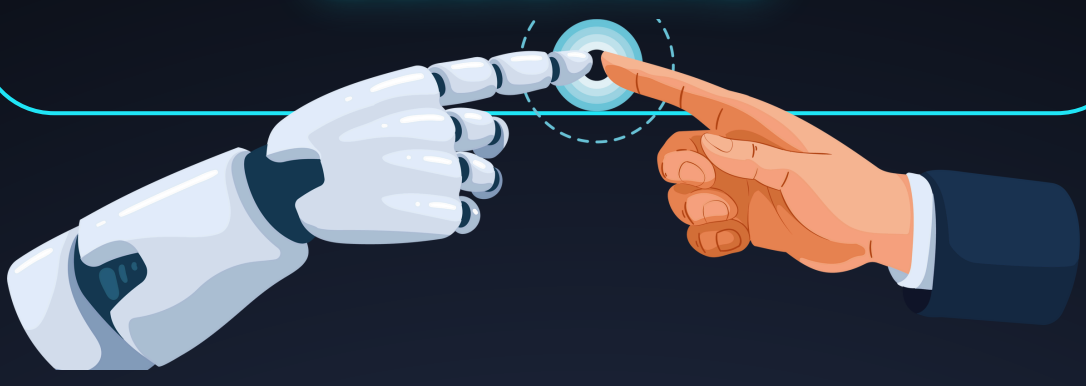
6 Redes sociales

No compartas información personal como tu dirección, teléfono o contraseñas. Revisa quién puede ver lo que publicas (configura la privacidad).

¡ Tú puedes protegerte !

Internet es un lugar increíble, pero hay que usarlo con precaución

BUENAS PRÁCTICAS PARA CREAR CONTRASEÑAS SEGURAS



LONGITUD ADECUADA

Utiliza contraseñas de al menos 12 caracteres; cuanto más largas, más seguras serán.

COMBINACIÓN DE CARACTERES

Incluye una mezcla de letras mayúsculas y minúsculas, números y símbolos especiales para aumentar la complejidad.

EVITA INFORMACIÓN PERSONAL

No uses datos fácilmente accesibles, como nombres, fechas de nacimiento o direcciones.

NO REUTILICES CONTRASEÑAS

Cada cuenta debe tener una contraseña única para evitar que una brecha de seguridad comprometa múltiples servicios

FRASES DE CONTRASEÑA

Considera usar frases de contraseña, combinando palabras aleatorias y símbolos, que sean fáciles de recordar, pero difíciles de adivinar.

GESTORES DE CONTRASEÑA

Utiliza herramientas especializadas para generar y almacenar contraseñas de forma segura, facilitando la gestión de múltiples credencialesL

AUTENTICACIÓN DE DOS FACTORES (2FA)

Habilita 2FA siempre que sea posible para añadir una capa adicional de seguridad

ACTUALIZACIONES PERIÓDICAS

Cambia tus contraseñas regularmente y especialmente si sospechas que han sido comprometidas

INFORMACIÓN Y CONSEJOS SOBRE CIBERSEGURIDAD. CURSO 2024-25

1

¿QUÉ ES EL 2FA?

La **Autenticación de Doble Factor (2FA)** es un sistema de seguridad que añade una segunda comprobación para entrar en una cuenta. Así, aunque alguien tenga tu contraseña, no podrá acceder sin el segundo paso.

2

¿CÓMO FUNCIONA?

Los factores de autenticación pueden ser:

✅ **Algo que sabes**: Una contraseña o un PIN.
✅ **Algo que tienes**: Un móvil, una tarjeta o una llave de seguridad.
✅ **Algo que eres**: Huella dactilar, rostro o voz.

💡 **Usa siempre dos factores diferentes, por ejemplo, contraseña + código en tu móvil.**

3

¿QUÉ MÉTODO DE 2FA ELEGIR?

Hay varios métodos de 2FA, pero no todos son igual de seguros:

🔹 **Más seguros:**
Aplicaciones como **Google Authenticator** o **Authy** y llaves físicas como **YubiKey**.
🔹 **Menos seguros:**
Códigos enviados por **SMS o correo electrónico** (pueden ser interceptados).
🔹 **Otros métodos:**
Huella dactilar o reconocimiento facial.

💡 **Elige apps de autenticación o llaves de seguridad en lugar de SMS.**

4

¿DÓNDE ACTIVAR 2FA?

Es importante activar **2FA en todas tus cuentas importantes**:

📧 **Correo electrónico** 💳 **Bancos y apps de pago**
📱 **Redes sociales** ☁️ **Almacenamiento en la nube**
🏢 **Cuentas del trabajo o la escuela**

💡 **Activa 2FA en todas tus cuentas importantes.**

5

¿CÓMO SABER SI 2FA FUNCIONA BIEN?

Cada cierto tiempo, revisa que **todo esté funcionando correctamente**:
🔹 Prueba que tu aplicación de autenticación genera códigos.
🔹 Intenta iniciar sesión en otra computadora para ver si 2FA funciona.
🔹 Asegúrate de no perder acceso a tu método de autenticación.

💡 **Haz pruebas cada pocos meses para evitar problemas.**

7

¿CÓMO PROTEGER LOS DISPOSITIVOS QUE USAS CON 2FA?

Si alguien accede a tu móvil u ordenador, podría robarte los códigos de 2FA. Para evitarlo:
🔹 Usa **contraseñas seguras** y de bloqueo de pantalla.
🔹 **No compartas tu dispositivo** con nadie.
🔹 Activa el **cifrado del móvil** para proteger tus datos

6

¿CÓMO RECUPERAR UNA CUENTA CON 2FA?

Si pierdes el acceso a 2FA, puedes recuperarlo con:
🔹 **Códigos de respaldo** (te los dan cuando activas 2FA).
🔹 **Correo de recuperación.**
🔹 **Contactando al soporte de la plataforma.**

💡 **Guarda los códigos de respaldo en un lugar seguro (no en tu móvil) y protege bien tu móvil.**

8

EVITA CAER EN ENGAÑOS Y ATAQUES

Los ciberdelincuentes intentarán robarte tus códigos de 2FA con trampas como:
❌ **Phishing** (mensajes falsos que piden tu código).
❌ **Páginas falsas** que parecen reales.
❌ **Personas que te piden códigos por WhatsApp o redes sociales.**

💡 **Nunca compartas tus códigos de 2FA con nadie.**

9

MANTÉN SEGUROS TUS DISPOSITIVOS

Para mejorar tu seguridad:
🔹 Mantén **actualizados** tus programas y apps.
🔹 Revisa **las configuraciones de seguridad** de tus cuentas.
🔹 Desactiva dispositivos que ya no uses.

💡 **Configura bien cada cuenta para evitar riesgos.**

10

NO USES MÉTODOS INSEGUROS

Add your text here

- Algunos métodos de 2FA pueden ser **hackeados fácilmente**:
  ❌ Los códigos por **SMS** pueden ser robados con ataques llamados **SIM swapping.**
  ✅ Es mejor usar **aplicaciones de autenticación o llaves de seguridad físicas.**

💡 **Evita los SMS y usa apps de autenticación siempre que sea posible.**

Activar **2FA** es una de las mejores maneras de **proteger tus cuentas.** Aunque parezca incómodo al principio, **impedirá que un hacker robe tu información.**

🔒 **¡Protege tu seguridad digital con 2FA!** 🔒

Identidad Digital

Información que **yo publico** + Información que **comparto** + Lo que **se dice de mí** = Información que **existe de mí** = **Mi identidad digital**

- **deja huella**
- **interviene** la actidad de terceras personas
- **es global**
- **influye** en la intercción
- **no se olvida**

Decálogo buenas práctica

1 PIENSA ANTES DE SUBIR CUALQUIER COSA

sé consciente de que finalmente cualquiera lo puede ver, aunque lo envíes a una sola persona

2 PARRTICIPA DE FORMA RESPUETUOSA

expresate con edución, ...

3 UTILIZA NOMBRES DE USUARIO O DE REGISTRO ADECUADO

nombre de usuario, correo

4 SELECCIONA CUIDADOSAMENTE LOS AVATARES E IMAGENES ASOCIADOS A TU PERFIL

5 CONOCE Y GESTIONA LA PRIVACIDAD DE LAS REDES DONDE PARTICIPAS

.

6 PRACTICA EGOSURFING

busca información de tí de forma regular

7 APORTA CONTENIDOS DE CALIDAD

.

8 RESPETA LOS DERECHOS DE AUTOR UY LAS LICENCIAS DE USO

9 SELECCIONA CON CUIDAD TUS AMISTADES

10 EJERCE LA CIUDADANÍA DIGITAL DE FORMA RESPONSABLE Y ACTIVA

denuncia actividaes ilicitas o inapropiadas

BIENESTAR DIGITAL

1 EQUILIBRIO TECNOLOGÍA Y VIDA PERSONAL

DESCONEXIÓN PROGRAMADA
Establecer horarios
ACTIVIDADES SIN PANTALLAS
Dedicar tiempo a hobbies no tecnológicos

2 USO CONSCIENTE DE LA TECNOLOGÍA

REDES SOCIALES
Limitar el tiempo en redes sociales.
NOTIFICACIONES
Desactivar notificaciones innecesarias.

3 SALUD FÍSICA Y ERGONOMÍA

POSTURA Y MOBILIARIO
Sentarse de manera que la pantalla quede a la altura de los ojos.
PAUSAS ACTIVAS
Hacer descansos regulares para estirarse y moverse

4 INTERACCIONES SOCIALES

COMUNICACIÓN RESPETUOSA
Practicar la empatía y el respeto hacia los demás
BALANCE ONLINE/OFFLINE
Equilibrar las interacciones en línea y cara a cara

CEPA Bernal Díaz del Castillo
Medina del Campo

SOBREEXPOSICIÓN EN LA RED

PROTEGE TU PRIVACIDAD

- Revisa y ajusta las configuraciones de privacidad
- Evita compartir detalles sensibles

SÉ CONSCIENTE DE LO QUE COMPARTES

- Piensa antes de publicar
- Evita la sobreexposición emocional

CONSIDERA LAS IMPLICACIONES LEGALES

- Infórmate sobre las leyes de protección de datos
- Sé. Consciente de los derechos de autor y la propiedad intelectural

CUIDA TUS IMÁGENES Y VÍDEOS

- Ten cuidado con las fotos y vídeos personales
- Piensa en las implicaciones de compartir imágenes

SÉ RESPONSABLE CON EL USO DE DATOS

- No compartas e información de otras personas sin su consentimiento
- Comprende el alcance de tus pulicaciones

GESTIONA LAS INTERACCIONES CON LOS DEMÁS

- Protege tu bienestar emocional
- Desactiva o bloquea cuentas y personas tóxicas

CONTROLA TU PRESENCIA EN REDES SOCIALES

- No compartas en exceso tu ubicación
- Evita conectar con desconocidos

ESTRATEGIAS PARA DETENER Y PREVENIR EL

Ciberacoso

¿Qué es el ciberacoso?

Es una forma de acoso que ocurre a través de medios digitales como redes sociales, mensajes de texto y correos electrónicos.

Tipos de ciberacoso

- **Insultos y humillaciones:** Mensajes ofensivos o degradantes.
- **Difusión de rumores:** Compartir información para dañar la reputación de alguien.
- **Exclusión de grupos:** Bloquear o excluir intencionadamente a alguien de comunidades digitales.

Impacto psicológico del ciberacoso

- **Ansiedad y depresión**: Provoca estrés, angustia y tristeza.
- **Baja autoestima:** Inseguridad y poca confianza en sí mismos.
- **Aislamiento social:** Evitar interacciones en línea y en la vida real.

Factores que contribuyen al ciberacoso

- **Anonimato:** Internet permite ocultar la identidad
- **Falta de empatía:** La distancia digital reduce la percepción del daño causado.
- **Presión de grupo:** Participar del ciberacoso para encajar en un círculo social.

Estrategias de prevención del ciberacoso

- **Educación:** Sensibilizar sobre los efectos negativos.
- **Supervisión:** Monitorear la actividad en línea y establecer normas de uso digital.
- **Comunicación:** Fomentar el diálogo abierto.

Marcos legales y denuncia

- **Leyes:** Normativas específicas para penalizar el ciberacoso.
- **Denuncia:** Reportar el acoso a plataformas digitales y autoridades competentes.
- **Protección**: Garantizar seguridad y justicia para las viíctimas.

Apoyo y Recursos para víctimas

- **Apoyo emocional:** Buscar ayuda en familiares amigos o profesionales.
- **Recursos en línea:** Utilizar líneas de ayuda y sitios web especializados.
- **Grupos de apoyo:** Compartir experiencias con otras víctimas.

BÚSQUEDA DE INFORMACIÓN SEGURA

Verificación de la Seguridad Web

-Candado en la barra de direcciones.
-Protocolo HTTPS
-Certificados SSL

Fuentes oficiales y confiables

-Sitios gubernamentales
-Instituciones académicas
-Organizaciones Internacionales

Expertos confiables

-Credenciales
-Reputación
-Publicaciones

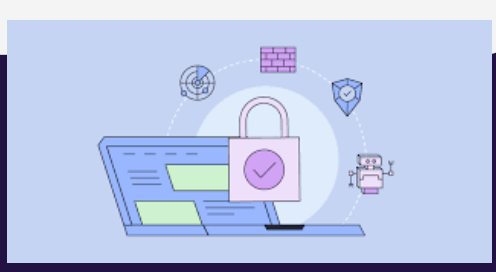
Consulta múltiples fuentes

-No te bases en una sola fuente.
-Busca consistencia.
-Evalúa la objetividad

Actualización de la información

-Fecha de publicación
-Información vigente
-Relevancia temporal

Crea un directorio de fuentes seguras



-Añade sitios de confianza.
-Mantén la lista actualizada.