coomuldesa
su respaldo financiero

Protegiendo el negocio en un mundo digital

COOMULDESA – SEGURIDAD DE LA INFORMACIÓN

En este material encontrarás sobre la importancia de la ciberseguridad en la protección de la información, los procesos y la confianza de nuestros asociados en la era digital.

Our Social Media
@coomuldesaoficial

More Information
www.coomuldesa.com

coomuldesa
su respaldo financiero

ENTENDIENDO LA SEGURIDAD DE LA INFORMACIÓN

🔐 ¿Qué es la Ciberseguridad?

La ciberseguridad es el conjunto de prácticas, procesos y herramientas diseñadas para proteger los sistemas, redes y datos de la cooperativa frente a accesos no autorizados, ataques cibernéticos y vulneraciones.

En Coomuldesa, entendemos que proteger la información es proteger a nuestros asociados, colaboradores y la confianza institucional.

Objetivos principales de la ciberseguridad

🔒 Confidencialidad

Asegurar que la información solo sea accesible por las personas autorizadas.

✅ Integridad

Garantizar que los datos no sean modificados de forma indebida, ya sea por error o ataque.

📅 Disponibilidad

Mantener los servicios y la información accesibles cuando se necesitan, sin interrupciones críticas.

🔍 Amenazas comunes en ciberseguridad

En la era digital, los ciberdelincuentes utilizan métodos cada vez más sofisticados para engañar a los usuarios y acceder a su información personal o financiera. En Coomuldesa queremos que estés alerta y te protejas de los siguientes riesgos:

🦠 MALWARE

Programas maliciosos que se instalan en tu dispositivo sin autorización, pueden robar información o dañar tus archivos.

🎣 PHISHING

Mensajes falsos (correos, SMS o enlaces) que simulan ser de entidades conocidas para pedirte datos personales o claves.

🔐 RANSOMWARE

Software que bloquea tu información y exige un pago para liberarla. Nunca pagues; repórtalo y busca ayuda técnica.

📞 VISHING

Llamadas telefónicas engañosas donde alguien se hace pasar por funcionario de una entidad para pedirte códigos, claves o datos.

coomuldesa
su respaldo financiero

⚠ Impactos del malware

Pérdida de información confidencial
puede robar claves, datos personales o financieros.

Interrupción de operaciones
bloquea el acceso a sistemas o archivos, afectando servicios clave.

Aumento de costos
implica gastos en recuperación, soporte técnico y fortalecimiento posterior.

Daño reputacional
genera desconfianza entre asociados y aliados si se compromete su información.

✅ ¿Cómo prevenir el malware?

- No abras archivos ni enlaces sospechosos, incluso si provienen de contactos conocidos.
- Mantén actualizado tu antivirus y el sistema operativo de tus dispositivos.
- Utiliza solo redes Wi-Fi seguras para ingresar a plataformas financieras.
- Descarga aplicaciones únicamente desde tiendas oficiales (App Store o Google Play).

¿Qué es el Phishing?

El phishing es una técnica de fraude digital en la que un ciberdelincuente se hace pasar por una entidad confiable (como una cooperativa, banco o red social) para obtener información confidencial del usuario. Usualmente se presenta como un mensaje por correo, SMS o red social que incluye enlaces maliciosos o solicitudes engañosas para que reveles datos como claves, números de tarjeta o códigos de verificación.

¿Cómo prevenir el phishing?

- Capacitación continua
- Activa filtros antiphishing y utiliza antivirus en tus dispositivos.
- Verificación del remitente. Coomuldesa nunca te solicitará claves o códigos por canales no oficiales.

coomuldesa
su respaldo financiero

¿Cómo prevenir un ataque de Ransomware?

El ransomware es un tipo de malware que bloquea el acceso a tus archivos o sistemas hasta que se pague un rescate. Prevenirlo es clave para proteger la continuidad del servicio, la confianza de los asociados y la integridad de la información, así que:

📧 No abras archivos adjuntos ni enlaces sospechosos, incluso si provienen de remitentes conocidos.
🔄 Mantén actualizado el sistema operativo y el antivirus en todos los equipos.

🎯 Impactos del ransomware

- **Pérdidas económicas**
- **Pérdida de información**
- **Interrupción operativa**
- **Daño reputacional**

☎️ ¿Qué es el Vishing?

El vishing es una modalidad de fraude telefónico en la que un estafador se hace pasar por funcionario de una entidad reconocida (bancos o autoridades) para obtener datos personales, claves, códigos de verificación o información financiera. Utilizan lenguaje convincente y situaciones urgentes para presionar a la víctima.

⚠️ **Ejemplo típico:**
“Se detectó una transacción sospechosa en su cuenta. Necesitamos validar su identidad con el código que le llegará por mensaje de texto”.

✅ ¿Cómo protegerse del vishing?

📵 No proporciones claves ni códigos por teléfono, si desconoce el origen de la llamada.

📲 Verifica siempre la identidad del remitente. Si tienes dudas, cuelga y llama directamente a los canales oficiales de Coomuldesa.

🗣️ Capacita a tu familia y equipo de trabajo para que reconozcan estos intentos de fraude.

📋 Reporta el intento inmediatamente a través de nuestros canales institucionales. Tu reporte puede evitar más víctimas.

Estrategia de Ciberseguridad – Coomuldesa

- **Evaluación de Riesgos**
- **Formación y Sensibilización**
- **Uso de Software de Seguridad**
- **Plan de Respuesta a Incidentes**

En Coomuldesa cuidamos tu información con una estrategia clara: evaluamos los riesgos para anticiparnos a posibles amenazas, capacitamos a nuestro equipo para que sepa cómo actuar, usamos programas de seguridad que protegen nuestros sistemas y tenemos un plan listo para responder rápido si ocurre algún incidente. Todo esto nos ayuda a proteger tu confianza y mantener seguros tus datos.