Manual de Seguridad en Internet Hogar y Empresarial

1. Seguridad en la red Wi-Fi

- **Cambia la contraseña por defecto del router**: nunca uses la que viene de fábrica.
- **Usa contraseñas largas y seguras** (mínimo 12 caracteres, con letras, números y símbolos).
- **Oculta el nombre de tu red (SSID)** si no necesitas que sea visible públicamente.
- **Actualiza el firmware del router** para corregir vulnerabilidades.
- **Divide la red en segmentos**: una para trabajo, otra para invitados, otra para dispositivos inteligentes.

Tip: No compartas tu contraseña principal con visitantes, usa la red de invitados.

2. Seguridad en equipos del hogar y la empresa

- **Mantén actualizado el sistema operativo y programas**.
- **Instala antivirus y firewall** para prevenir accesos no autorizados.
- **Haz copias de seguridad periódicas** en discos externos o servicios en la nube.
- **Configura cuentas de usuario separadas** en los equipos compartidos.
- **Desactiva el inicio automático de dispositivos USB** para evitar malware.

3. Prevención de fraudes en internet

- **Correos sospechosos:** no abras enlaces ni adjuntos de remitentes desconocidos.
- **Mensajes falsos:** desconfía de supuestos premios o alertas urgentes.
- **Webs fraudulentas:** revisa que la dirección comience con https:// y tenga candado en el navegador.
- **Pagos en línea:** usa plataformas seguras y evita ingresar datos en sitios poco confiables.

Tip: Si recibes un correo que parece de tu banco, entra directamente a la página oficial escribiendo la dirección en el navegador, nunca desde un enlace recibido.

4. Buenas prácticas en empresas

- **Políticas de contraseñas:** exigir cambios periódicos y uso de claves seguras.
- **Capacitación a empleados:** enseñar a reconocer correos y sitios fraudulentos.
- **Accesos controlados:** limitar permisos según el rol de cada persona.
- **Monitoreo de la red:** usar herramientas que detecten accesos extraños.
- **VPN para trabajo remoto:** protege la conexión de empleados fuera de la oficina.

5. Qué hacer si sospechas de un ataque

1. **Desconecta el equipo de la red** para evitar propagación.
2. **Guarda evidencia** (capturas de pantalla, correos, mensajes).
3. **Informa al responsable de TI** en empresas o busca ayuda técnica en el hogar.
4. **Restaura desde una copia de seguridad** si es necesario.

6. Checklist rápido

- [ ] Cambié la contraseña del router.
- [ ] Mis equipos tienen antivirus y firewall activos.
- [ ] Realizo copias de seguridad periódicas.
- [ ] Sé identificar correos y sitios sospechosos.
- [ ] En la empresa, hay políticas claras de seguridad.