**DETALLES DE LAS CÁPSULAS EN VIDEO**

**Cápsula Nro 1: "Conviértete en el Primer Escudo de Ciberseguridad"**

Objetivo: Resaltar la importancia de la participación activa de los usuarios finales en la seguridad de la información.

**TIPs para ser el Primer Escudo de Ciberseguridad:**

1. **No compartas tus contraseñas**: Mantén tus credenciales seguras y nunca las divulgues, ni siquiera a colegas o amigos.
2. **Usa contraseñas seguras**: Crea contraseñas complejas que incluyan letras, números y símbolos. Utiliza un gestor de contraseñas para almacenarlas de manera segura.
3. **Piensa antes de hacer clic**: Desconfía de correos electrónicos y mensajes no solicitados. Si algo parece sospechoso, no abras enlaces o archivos adjuntos.
4. **Reporta actividades sospechosas**: Si ves algo inusual en tu cuenta o dispositivo, avisa inmediatamente al equipo de TI o seguridad de la empresa.
5. **Desconfía de solicitudes de información personal**: Nunca compartas datos personales o corporativos sensibles a través de correos electrónicos o llamadas telefónicas no verificadas.
6. **Sé escéptico de las ofertas demasiado buenas**: Los cibercriminales utilizan correos electrónicos y anuncios falsos para tentar a los usuarios. Si parece demasiado bueno para ser verdad, probablemente sea una estafa..
7. **Sé consciente del phishing**: Los correos de phishing se disfrazan de comunicaciones legítimas. Revisa cuidadosamente las direcciones de correo y los enlaces antes de actuar.
8. **Protege tu información personal en redes sociales**: Configura la privacidad en tus redes sociales para controlar quién tiene acceso a tu información sensible.

**Cápsula Nro 2. "La Importancia del Uso Seguro de la Tecnología"**

Objetivo: Concienciar sobre el uso seguro de las herramientas tecnológicas dentro de la empresa.

**TIPs para un uso seguro de la tecnología:**

1. **Ten cuidado con el Wi-Fi público**: Evita acceder a información confidencial o realizar transacciones en redes Wi-Fi públicas sin usar una red privada virtual (VPN).
2. **Bloquea tu dispositivo cuando no lo uses**: Asegúrate de bloquear tu computadora o teléfono cuando te alejes de ellos, aunque sea por un momento.
3. **Haz respaldos regulares**: Realiza copias de seguridad de tus datos importantes en ubicaciones seguras y externas. Te protegerá contra ataques como el ransomware.
4. **Cierra sesiones después de usarlas**: No te olvides de cerrar tus sesiones, especialmente en dispositivos compartidos o públicos.
5. **No descargues aplicaciones sin verificar**: Instala software únicamente de fuentes confiables y oficiales para evitar malware o programas maliciosos.
6. **Desactiva el Bluetooth cuando no lo uses**: Mantén apagado el Bluetooth y otros servicios inalámbricos cuando no sean necesarios, para evitar posibles accesos no autorizados.
7. **Ten cuidado con los dispositivos USB externos**: Asegúrate de que estén libres de virus antes de conectarlos a tu computadora. Utiliza solo dispositivos USB verificados.
8. **Haz un uso responsable de los recursos de la empresa**: Utiliza los dispositivos y herramientas tecnológicas de la empresa únicamente para fines laborales y sigue las políticas de uso de recursos tecnológicos.

**Cápsula Nro. 3. "La Ciberseguridad es Colaboración: Juntos Fortalecemos la Defensa"**

Objetivo: Promover una cultura colaborativa de ciberseguridad en la empresa.

**TIPs para mejorar la colaboración interna en Ciberseguridad:**

1. **Comparte información sobre amenazas**: Si descubres o te enfrentas a un ataque cibernético o actividad sospechosa, informa de inmediato al equipo de TI. La detección temprana ayuda a prevenir daños mayores para todos.
2. **Sigue las políticas de seguridad de la empresa**: Colabora cumpliendo con las normativas y procedimientos de seguridad establecidos, como el uso adecuado de contraseñas, la clasificación de información, y el manejo de dispositivos.
3. **Apoya la cultura de seguridad**: Fomenta conversaciones abiertas sobre ciberseguridad con compañeros de trabajo y familiares. Cuanto más conscientes y educados estemos todos, más protegidos estaremos como equipo.
4. **Sé un modelo de buenas prácticas**: Los demás aprenderán de tu ejemplo. Cumple con los protocolos de seguridad de la información y muestra el camino a quienes tienen menos experiencia en temas de ciberseguridad.
5. **Denuncia comportamientos inseguros**: Si observas malas prácticas, como el uso de contraseñas débiles o el acceso a sitios no confiables, informa de manera constructiva para que todos puedan corregir y mejorar.
6. **Participa en capacitaciones y simulacros**: Aprovecha las sesiones de formación y simulacros de ciberseguridad que la empresa o instituciones organizan. Una buena preparación y un equipo capacitado son la primera defensa ante ciberataques.
7. **Colabora para identificar vulnerabilidades**: Trabaja junto al equipo de TI informando sobre cualquier vulnerabilidad o área de mejora que encuentres en los sistemas o procesos tecnológicos, sin temor a señalar posibles fallos.
8. **Protege la información de tus compañeros**: Asegúrate de tratar con responsabilidad la información personal o confidencial de otros miembros de la empresa, protegiéndola con la misma diligencia que tus propios datos.