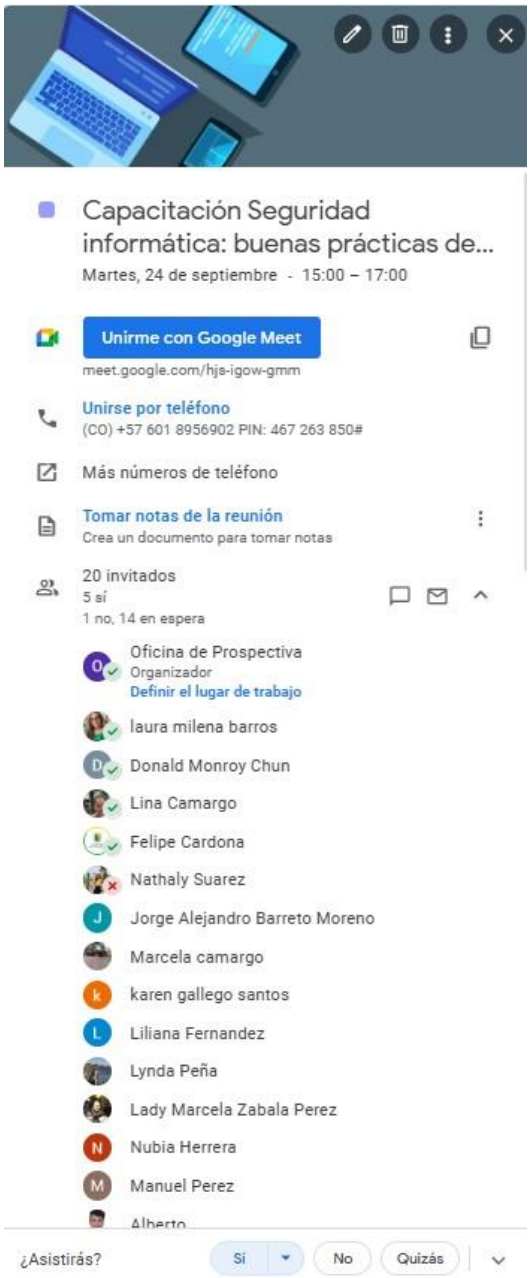
Soporte: Capacitación TICs
Seguridad Informática: buenas prácticas en ciber seguridad

Fecha: Martes 24 de septiembre de 2024.
Liderada por: Dirección de Tics
Invitación:



Notas:

Seguridad Informática:
- Confidencialidad: Protección de datos sensibles y accesos no autorizados.
- Integridad: Aseguramiento de que los datos no han sido alterados indebidamente.
- Disponibilidad: Garantizar que los sistemas y datos estén disponibles para usuarios legítimos.

Ciberseguridad:
- Subconjunto de la seguridad informática, enfocado en sistemas conectados a internet.
- Protección de Redes: Uso de cortafuegos y programas de seguridad.
- Seguridad en Aplicaciones: Protección del software contra vulnerabilidades.
- Gestión de Riesgos: Identificación y evaluación de amenazas potenciales.
- Criptografía: Uso de técnicas para proteger información durante la transmisión y almacenamiento.
- Respuesta a Incidentes: Planes de contingencia y recuperación ante ataques.
- Amenazas Persistentes: Ataques sofisticados dirigidos a organizaciones de alto perfil.

Amenazas Comunes:
- Phishing: Fraude donde atacantes se hacen pasar por entidades confiables para obtener información personal.
- Malware y Ransomware: Software dañino que puede bloquear acceso a archivos hasta que se pague un rescate.
- Ingeniería Social: Manipulación de personas para que revelen información confidencial.
- Ataques DDoS: Intentos de hacer que un sitio web no esté disponible inundándolo con tráfico falso.

Buenas Prácticas de Ciberseguridad:
- Contraseñas Fuertes: Uso de contraseñas complejas y únicas para cada cuenta.
- Actualizaciones y Parches: Mantener el software actualizado para evitar vulnerabilidades.
- Autenticación Multifactor: Añadir capas adicionales de seguridad.
- Navegación Segura: Verificar que las URLs comiencen con "https".
- Copias de Seguridad: Realizar copias de seguridad regularmente y almacenarlas en diferentes lugares.

Soporte: Capacitación TICs

Seguridad Informática: buenas prácticas en ciber seguridad

Plan de Respuesta a Incidentes:

- Identificación del Problema: Detectar correos sospechosos y actividad inusual.
- Acción Rápida: Desconectar sistemas afectados para contener el ataque.
- Notificación: Informar a empleados y clientes sobre el incidente.
- Equipo de Respuesta: Tener un equipo capacitado en ciberseguridad.
- Documentación y Aprendizaje: Documentar el incidente y aprender de él.
- Recuperación de Datos: Realizar copias de seguridad y pruebas de recuperación.

Conclusión:

- La ciberseguridad es una responsabilidad compartida que requiere un enfoque integral, incluyendo tecnologías, procesos y personas.
- La prevención y la educación son claves para proteger la información y mitigar riesgos.

Registro fotográfico



Soporte: Capacitación TICs

Seguridad Informática: buenas prácticas en ciber seguridad

