- SEMANA 8 HOJA DE REFERENCIA: Política de escritorio limpio -

IDEAS PRINCIPALES	NOTAS
¿Qué es una política de escritorio limpio?	Una política de escritorio limpio asegura que todos los documentos importantes, cartas confidenciales, carpetas, libros, etc., sean retirados de un escritorio y guardados bajo llave cuando los artículos no están en uso o un/a empleado/a deja su puesto de trabajo. **Es una de las principales estrategias que se debe utilizar cuando se trata de reducir el riesgo de vulnerar la seguridad de nuestra información.** Tener un escritorio limpio nos ayuda dos maneras importantes: • elimina el desorden • ayuda a prevenir la probabilidad de que alguien pueda acceder a la información de su empresa o a la información de sus clientes. **La Política de un escritorio limpio trata de ayudarle a estar consciente de su valiosa información y las amenazas a la que ésta está expuesta.**
Amenazas externas que ponen a su información en peligro	Cuatro de las mayores amenazas externas en contra de nuestras organizaciones hoy en día son:  Phishing Ingeniería social Ransomware WiFi inseguro
PHISHING	
¿Qué es Phishing?	El phishing se refiere a la práctica de crear correos electrónicos falsos que aparentan provenir de alguien en quien usted confía, algunos ejemplos incluyen: • Instituciones bancarias • Organizaciones que ofrecen tarjetas de crédito • Sitios web populares El correo electrónico le pedirá que: 1. *"confirme los detalles de su cuenta o los detalles de la cuenta de su proveedor"* 2. posteriormente, le dirigirá a un sitio web que se parece al verdadero, pero cuyo único propósito es robar su información.

INGENIERÍA SOCIAL	
¿Qué es ingeniería social?	• Cuando se intenta robar información o la identidad de una persona, un hacker en lugar de entrar en su computadora a menudo intenta engañarle para que usted proporcione información confidencial. • Al poner un cebo o carnada - Por teléfono - Por mensaje de texto - Correo electrónico (También llamado phishing)
Ingeniería Social - Tácticas por teléfono	PASO 1: Es posible que reciba una llamada de alguien que se hace pasar por un/a empleado/a de Microsoft. *(Una organización popular. Lo más probable es que esté usando algún tipo de software de Microsoft).* PASO 2: La persona intenta ganarse su confianza asustándole e informándole que puede protegerle. *(Por ejemplo, afirma que ha recibido un mensaje que indica que su equipo está en peligro o comprometido* *y que tiene que iniciar sesión en su sistema para arreglarlo.)* PASO 3: Una vez que usted le proporciona el acceso, la persona instalará un virus real en su computadora y le pedirá que le pague para que pueda eliminarlo. Si usted se niega a pagar, intentará activar el virus que ha instalado en su computadora para destruirla y así vengarse de usted.
RANSOMEWARE	
¿Qué es el Ransomware?	El Ransomware es un tipo de malware (software malicioso) que los delincuentes usan para extorsionar dinero. Este software retiene los datos para el rescate utilizando la encriptación o bloqueando a los usuarios fuera de su dispositivo. • A menudo, los sistemas se infectan por el ransomware a través de un enlace en un correo electrónico malicioso. • Cuando el usuario hace clic en el enlace, el ransomware se descarga en la computadora, el teléfono inteligente u otro dispositivo del usuario. • El ransomware puede propagarse a través de redes conectadas.
WIFI NO SEGURO	

¿Qué es un WiFi no seguro?	Una conexión **Wi-Fi** no segura es aquella que no utiliza ningún tipo de encriptación de seguridad. Los canales Wi-Fi encriptados aseguran sus datos contra la interceptación, ya que nadie puede acceder a ninguno de las computadoras conectados o a la propia conexión.
Riesgos de un WiFi no seguro	El mayor riesgo de conectarse a una conexión Wi-Fi no segura proviene del uso de servicios que requieren información de acceso. Los datos transmitidos a través de Wi-Fi no seguro pueden ser interceptados por terceros. Estos terceros pueden extraer su información de inicio de sesión y sus contraseñas de estos datos interceptados y utilizarlos para acceder a sus servicios de forma fraudulenta.
Solución al uso de WiFi no seguro	Sólo hay una solución a las amenazas de usar redes inalámbricas no seguras... ***No las use.*** Si necesita acceso a la red, sólo active la función de hotspot en tu teléfono móvil y úsela como WiFi.
RECOMENDACIONES DEL ADMINISTRADOR DE CONTRASEÑAS	
Tres de los mejores administradores de contraseñas recomendados	DASHLANE LastPass **** 1Password
DASHLANE	*Lo que diferencia a Dashlane de sus competidores es su Cambiador de Contraseñas, que* ***reemplaza cientos de contraseñas con un solo clic.*** *Esta característica increíblemente útil, que es sorprendentemente rara en el mundo de los administradores de contraseñas, ahorra mucho tiempo y está disponible tanto para los usuarios que adquieren los servicios gratuitos o adquieren un servicio premium.*
LAST PASS	*LastPass Free es el mejor administrador de contraseñas gratuito disponible.* ***No le restringe a un solo dispositivo o a un número específico de contraseñas****. Lo mejor de todo es que viene con características adicionales que son muy útiles, como la función de Reto de Seguridad (Security Challenge)- que monitorea la resistencia de la contraseña - y el sistema 2FA incorporado – el autenticador LastPass.*
1PASSWORD	*1Password tiene el mejor plan familiar en términos de precio y se pueden compartir los datos de manera segura - hace que compartir datos importantes con su familia sea sumamente fácil. La función Watchtower envía alertas si alguna credencial ha sido vulnerada, y el 2FA incorporado añade otra poderosa capa de seguridad a un gestor de contraseñas ya seguro. Además, con una prueba gratuita de 30 días, puede comprobarlo y ver si es adecuado para usted y su familia.*