Lista de comprobación de contraseñas

☐ Utilice siempre una contraseña o frase de contraseña segura

- ☐ **Cambie siempre las contraseñas predeterminadas** antes del primer uso
- ☐ **Utilice una frase de contraseña de al menos 15 caracteres para crear sus contraseñas.** Una frase de contraseña es parte de una oración, como "**VacacionesFavoritasPirineos**" o una oración, como "Me gusta el baloncesto".
- ☐ **Verifique la seguridad de las contraseñas** antes de usarlas

☐ Use una contraseña diferente para cada cuenta

- ☐ Asegúrese de que **cada cuenta usa una contraseña/frase de contraseña segura diferente**/que sea **completamente impersonal o generada aleatoriamente**
- ☐ **NO use fórmulas** para crear contraseñas "únicas" para sus cuentas: son fáciles de recordar pero igualmente fáciles de descifrar (PasswordFB, PasswordYT, PasswordGmail, etc.)

☐ Active la autenticación multifactor

- ☐ Active la autenticación multifactor en todas sus cuentas, siempre que sea posible

☐ Consejos de seguridad de contraseñas

- ☐ **Elimine cuentas y desinstale aplicaciones** que ya no usa
- ☐ **Asegúrese de que todas sus cuentas utilicen contraseñas seguras** y que no se utilizan contraseñas más de una vez
- ☐ Verifique la configuración de seguridad en sus dispositivos conectados, cuentas y aplicaciones para ver la configuración actual o predeterminada existentes
- ☐ **Verifique la seguridad de sus contraseñas actuales y actualícelas** según sea necesario
- ☐ **Nunca revele las contraseñas de la empresa a nadie.** Aplique siempre nuevas contraseñas antes y después de cualquier viaje en el que se utilicen datos de la empresa en un dispositivo

Lista de verificación de actualización de software

☐ Descargar y activar actualizaciones automáticas

Asegúrese de que todos sus sistemas, aplicaciones y dispositivos tengan los parches aplicados y estén configurados para las actualizaciones automáticas

- ☐ **Productos de Apple** - Productos y software de iPhone, iPad, Apple Watch o macOS
- ☐ **Productos de Android** - Cualquier dispositivo, aplicación o sistema con tecnología Android (puede incluir: smartphones, ordenadores portátiles, tabletas, relojes inteligentes, electrodomésticos, automóviles, sistemas domésticos inteligentes y supervisión de seguridad, cámaras, televisores inteligentes, consolas de juegos)
- ☐ **Productos de Microsoft** - Sistemas operativos Windows: ordenadores portátiles, ordenadores de sobremesa, tabletas, smartphones, consolas de juegos y más
- ☐ **Otras aplicaciones/plataformas/dispositivos** - Aplique parches y configure las actualizaciones automáticas en todos los demás dispositivos y aplicaciones (es decir, la suite Office365 en un **Mac**)

☐ Haga que las actualizaciones de software sean una práctica habitual

Hemos agregado una política de software del Programa de preparación cibernética al manual de estrategias del empleado, en la que se describen las expectativas en torno a las actualizaciones de software y otros problemas importantes de seguridad.

- ☐ Active las notificaciones de actualizaciones automáticas y no las ignore
- ☐ Instale las actualizaciones de software tan pronto como pueda, idealmente dentro de las 24 horas
- ☐ Mantenga siempre actualizados los dispositivos comerciales y personales que usa para el trabajo

Lista de comprobación para la concienciación sobre el phishing

Manténgase alerta y use esta lista de verificación para determinar rápidamente si un mensaje extraño podría ser un ataque de phishing.

4 formas de detectar un phish

1. Verifique el encabezado

- ☐ ¿Le he dado mi dirección de correo electrónico a esta empresa antes?
- ☐ ¿Tengo una cuenta con esta empresa?
- ☐ ¿La identidad del remitente coincide con la finalidad del correo electrónico?
- ☐ ¿Mi correo electrónico está en la lista de direcciones De:?
- ☐ ¿La dirección Para: está dirigida a destinatarios no revelados o a un gran número de destinatarios que no conoce?

2. Verifique el contenido

- ☐ ¿Los enlaces proporcionados en el cuerpo del correo electrónico parecen válidos?
- ☐ ¿Hay errores ortográficos y tipográficos? ¿Cómo es la gramática y el tono apropiado?
- ☐ ¿Me están prometiendo mucho dinero a cambio de poco o ningún esfuerzo por mi parte?
- ☐ ¿Se me pide que aporte dinero por adelantado para actividades dudosas, una tasa de tramitación o que pague el coste de agilizar el proceso?
- ☐ ¿Alguien me pide mi número de cuenta bancaria, otros datos financieros personales o contraseñas? (“Verifique su cuenta” o “Haga clic en el enlace a continuación para obtener acceso a su cuenta” son comunes)

3. Considere la finalidad del correo electrónico

- ☐ ¿El problema realmente es tan urgente como lo hace ver el remitente?
  - ☐ “Si no responde en 48 horas, su cuenta se cerrará”.
  - ☐ “Si no lo hace, es posible que su cuenta se desactive automáticamente”.
- ☐ ¿Por qué el remitente solicita confidencialidad? ¿Cómo puedo saber si la actividad propuesta es legítima y auténtica?

4. Tenga cuidado con los archivos adjuntos

- ☐ No abra archivos adjuntos inesperados.
- ☐ No abra archivos adjuntos de extraños. Asegúrese siempre de conocer primero al remitente
- ☐ No abra archivos adjuntos inusuales.
- ☐ No abra archivos adjuntos que vengan con mensajes de apariencia extraña.

Lista de verificación de unidades multimedia extraíbles USB

Siga estas pautas para usar y gestionar unidades y dispositivos multimedia extraíbles en el trabajo

Cuándo usar:

- ☐ **NO use unidades USB sin permiso previo** para el trabajo o en el trabajo
- ☐ **Evite usar unidades multimedia extraíbles** en la medida de lo posible
  - ☐ Si actualmente está utilizando unidades USB para su puesto, trabaje con las personas adecuadas para transferir de forma segura todos los datos confidenciales a una unidad segura y elimine de inmediato los datos del dispositivo después de terminar.
- ☐ **Nunca conecte dispositivos multimedia desconocidos que haya encontrado** en un ordenador. Entregue cualquier dispositivo de almacenamiento desconocido al personal de seguridad o de TI.

Cómo protegerse:

- ☐ **Desactive las funciones de ejecución automática y reproducción automática** para todas las unidades o dispositivos multimedia extraíbles. Estas funciones se ejecutan automáticamente cuando se conectan a un puerto o unidad USB.
- ☐ **Asegúrese de que las soluciones antivirus estén instaladas** en su ordenador para analizar activamente malware cuando se conecte cualquier tipo de unidad o dispositivo multimedia extraíble.
- ☐ **Asegúrese de que todas las unidades y dispositivos multimedia extraíbles estén cifrados.** Esto hará que los datos sean inútiles para los usuarios no autorizados en caso de pérdida o robo del dispositivo.
- ☐ **Aplique siempre nuevas contraseñas antes y después de cualquier viaje** donde se utilizan datos de la empresa en unidades o dispositivos multimedia extraíbles. Nunca revele las contraseñas utilizadas con unidades o dispositivos multimedia extraíbles.
- ☐ **Mantenga separados los datos personales y comerciales.** No almacene datos de trabajo en ningún dispositivo personal y viceversa