Consejos y recomendaciones

Mantenga unos buenos hábitos de seguridad en línea con estos consejos y recomendaciones. La presente sección se ha elaborado en coordinación con Get Safe Online (Reino Unido) y el Departamento de Seguridad Nacional (Estados Unidos).

- Proteja su ordenador personal (PC) y sus dispositivos portátiles
- Proteja su información personal y su identidad
- Proteja la información empresarial cuando se encuentre fuera de la empresa
- Conéctese de forma segura
- Sea prudente en Internet

Proteja su ordenador personal (PC) y sus dispositivos portátiles

PC

- Utilice un cortafuegos: sirven para protegen su red de algunos virus y de los piratas informáticos.
- Instale programas antivirus: impiden que las infecciones causadas por virus informáticos se propaguen por su ordenador.
- Adquiera las últimas actualizaciones de seguridad: mantenga sus aplicaciones y el sistema operativo en forma, saludables y al día.
- Impida la entrada de programas espía: no permita que se introduzcan en su ordenador elementos extraños rechazando los mensajes de correo electrónico y archivos adjuntos sospechosos.
- Realice copias de seguridad con regularidad: proteja sus datos frente a desastres.

Ordenadores portátiles

- Apague las conexiones inalámbricas cuando no las esté utilizando o no sean necesarias.
- Conecte periódicamente su ordenador portátil a una red fiable para actualizar sus mecanismos de seguridad.
- Realice copias de seguridad de la información que almacene en su ordenador portátil.
- Vigile en todo momento su ordenador portátil.

Unidades USB

- Utilice unidades USB cifradas.
- Ponga la unidad flash USB en modo de solo lectura utilizando el interruptor físico para evitar la transmisión de virus: algunas unidades flash USB incluyen un interruptor que

permite poner el dispositivo en modo de solo lectura y así evitar que el ordenador principal *(host)* pueda introducir o modificar datos en la unidad

- Realice una exploración de la unidad flash USB después de copiar archivos de un equipo no fiable y/o no autorizado, para evitar que se introduzcan virus.
- Antes de conectar su unidad USB en el ordenador de otra persona, elimine todos los archivos que no estén relacionados con esa acción.
- Realice una copia de seguridad de la información almacenada en su USB para que pueda recuperar los datos en caso de que se produzca un desastre.
- Coloque unidades USB en llaveros/cordones de colgantes para evitar su pérdida: el reducido tamaño de las unidades flash USB facilita su pérdida o robo. Por otra parte, cuanta mayor capacidad de almacenamiento tienen, mayor es la cantidad potencial de datos que corren el riesgo de ser objeto de acceso no autorizado. Las unidades flash USB suelen llevarse en bolsos, mochilas, fundas de ordenadores portátiles, chaquetas, bolsillos de pantalones o se dejan sobre la mesa de trabajo sin vigilancia. Últimamente ha aumentado el número de incidentes por unidades USB extraviadas, colocadas en lugares que no les corresponde, tomadas prestadas sin autorización o robadas.

Teléfonos móviles y equipos de bolsillo

Los equipos de bolsillo como Windows Mobile, Palm, iPhone, Android y Blackberry permiten acceder a Internet y tienen la capacidad de almacenar una gran cantidad de información. El mero hecho de ser portátiles exige una precaución adicional

- Apague las conexiones inalámbricas (es decir, Bluetooth y WLAN) cuando no las utilice. La tecnología Bluetooth permite a los dispositivos electrónicos comunicarse entre sí a través de un enlace de radio de corto alcance.
- No deje su teléfono móvil ni su dispositivo de bolsillo sin vigilancia. De lo contrario, podría dar lugar a pérdidas de datos.
- Use la función de contraseña para evitar que se produzcan accesos remotos no autorizados a su teléfono inteligente.

Proteja su información personal y su identidad

- **Utilice una contraseña segura**: la contraseña en Internet es el equivalente a la llave y la cerradura de su casa. Las contraseñas son una defensa de primer orden, y mantener buenas prácticas en relación con ellas le ayudará a aumentar la seguridad de su información personal y su identidad. La contraseña de su ordenador es la llave para acceder a toda la información –tanto empresarial como personal– que haya almacenado en su equipo y sus cuentas en línea. Utilice una contraseña segura para proteger los datos: procure que esté formada por un conjunto complejo de caracteres, que incluya letras (mayúsculas y minúsculas), números y símbolos. Cuanto más variados sean los caracteres incluidos en su contraseña, más difícil resultará descubrirla. No utilice información personal –su nombre, el

nombre de su hijo, fechas de nacimiento, etc.– que alguna persona pueda conocer o averiguar fácilmente, e intente evitar palabras comunes: algunos piratas informáticos utilizan programas que prueban con cada una de las palabras del diccionario.

- **Cambie su contraseña con regularidad**: si cree que su sistema ha estado en peligro, cambie las contraseñas de inmediato.
- **Mantenga en secreto sus contraseñas**: las contraseñas son únicas y no se deben comunicar a nadie. Siempre que sea posible, intente aprendérselas de memoria. Búsquese una estrategia para memorizarlas. Si escribe sus contraseñas, tenga cuidado con el lugar en el que vaya a guardar esta información; no la deje en sitios en los que no dejaría la información que protegen.
- **Cuenta única, contraseña única**: utilice contraseñas distintas para cada una de las cuentas en línea a las que tenga acceso (o, al menos, varias contraseñas). Si utiliza las mismas contraseñas en varias cuentas, un ciberdelincuente que acceda a una de ellas tendrá la puerta abierta a todas las demás.
- **Proteja sus cuentas**: muchos proveedores de cuentas ofrecen modos adicionales de verificar quién es el usuario antes de que éste realice operaciones empresariales en ese sitio.
- **Controle su presencia en línea**: siempre que sea posible, establezca parámetros de intimidad y seguridad en los sitios web de acuerdo con el nivel con el que desee facilitar información. Es preferible establecer límites en relación con las personas con las que se intercambia información.
- **Utilice con precaución los sitios de redes sociales**: tenga en cuenta que estos sitios pueden congregar muchos de los riesgos asociados a estar en línea: intimidación en línea, divulgación de información privada, ciberacoso, acceso a contenidos inadecuados para determinadas edades y, en el caso más extremo, captación y abuso de menores en línea.

Proteja la información empresarial cuando se encuentre fuera de la empresa

- **Asegúrese de que mantiene segura la información sensible**: cuando se encuentre fuera de su empresa, asegúrese de que mantiene la información sensible y los equipos seguros en todo momento para evitar la pérdida o el robo. Cuide la información, en especial cuando esté en lugares públicos.
- **Mantenga la confidencialidad de la información empresarial**: tenga presente que alguien puede escuchar por casualidad la conversación que mantiene usted. No deje que cualquiera pueda acceder a la información confidencial de su empresa.
- **Tenga cuidado de que ninguna persona situada cerca de usted pueda «espiar» lo que hace usted en su equipo:** mientras viaje o trabaje desde un lugar distante, proteja su información de este tipo de acciones.
- **Utilice el correo web con precaución**: la utilización de un navegador de Internet para leer su correo exige la misma precaución que si se tratara del sistema de correo de su ordenador, y entraña además sus propios riesgos para la seguridad.

Conéctese de forma segura

- **Apague las conexiones inalámbricas cuando no las esté utilizando o no sean necesarias.**
- **Utilice con inteligencia las zonas de conexión Wi-Fi**: cuando se encuentre en una zona Wi-Fi, limite el tipo de actividad empresarial que realiza y ajuste las configuraciones de seguridad en su dispositivo para seleccionar quién puede acceder a su equipo.
- **Proteja su dinero**: al realizar operaciones bancarias y compras en línea, verifique que los sitios tienen habilitados sistemas de seguridad. Busque direcciones web que empiecen por «https://» o bien «shttp://», que significa que el sitio adopta medidas adicionales para contribuir a proteger su información. «http://» no es seguro.
- **Elimine el correo electrónico no deseado**: este tipo de mensajes, también denominados *«spam»*, representan una amenaza para la seguridad. No abra los mensajes ni los archivos adjuntos de desconocidos.
- **En caso de duda, elimínelo**: cuando los vínculos de mensajes de correo electrónico, *tweets* y anuncios publicitarios en línea le resulten sospechosos, aunque sepa de quién proceden, es mejor suprimirlos o, si procede, marcarlos como «correo basura».
- **Reenvíe los mensajes de correo electrónico solo si es apropiado**. Antes de hacerlo, no obstante, considere la posibilidad de eliminar la historia del mensaje.
- **Navegue por Internet con cuidado.**
- **No descargue documentos y material de sitios no fiables.**
- **Utilice ordenadores públicos con precaución:** conéctese a un ordenador público solo cuando tenga una conexión cifrada (en tal caso, en la parte inferior derecha de la ventana de su navegador debe aparecer un candado, y las letras «https://» al principio de la dirección del sitio web).
- **Utilice los servicios de correo web que ofrecen empresas conocidas y de confianza.**

Sea prudente en Internet

- **Manténgase al día:** no deje de actualizar sus conocimientos sobre los nuevos modos de conservar la seguridad en línea: Busque en sitios web fiables la información más actualizada, compártala con sus familiares, amigos y compañeros, y anímeles a ser prudentes en Internet. Mantenga su navegador seguro.
- **Piense antes de actuar**: tenga cuidado con las comunicaciones que le indican que actúe de inmediato, que ofrezcan algo que parece demasiado bueno para ser cierto o que soliciten información personal.
- **Haga copias de seguridad**: proteja su trabajo, su música, sus fotografías y cualquier otra información digital realizando una copia electrónica y almacenándola de forma segura.