

# Contents

<b>1</b>	<b>Manual de seguridad</b>	<b>1</b>
1.1	Contenido . . . . .	1
<b>2</b>	<b>políticas para la estabilidad de los datos confidenciales</b>	<b>2</b>
2.1	Ataques de phishing . . . . .	2
2.2	Entrenamiento dirigido . . . . .	3
2.3	Seguridad en el hogar . . . . .	3
<b>3</b>	<b>Medios extraíbles</b>	<b>6</b>
3.1	Contraseñas y autenticación . . . . .	6
3.2	Manejo de correo electrónico e internet . . . . .	7
<b>4</b>	<b>Seguridad física</b>	<b>7</b>
4.1	Seguridad de los dispositivos móviles . . . . .	7
4.2	Trabajar a distancia . . . . .	8
4.3	Wi-Fi público . . . . .	8
<b>5</b>	<b>Seguridad en la nube</b>	<b>9</b>
5.1	Uso aceptable del equipo . . . . .	9
5.2	Uso seguro del navegador . . . . .	10
5.3	Protección de Datos . . . . .	10
<b>6</b>	<b>Informar incidentes</b>	<b>10</b>

## 1 Manual de seguridad

### 1.1 Contenido

Ataques de phishing. Medios extraíbles. Contraseñas y autenticación.  
Manejo de correo electrónico e internet.  
Seguridad física.  
Seguridad de los dispositivos móviles. Trabajar a distancia. Wi-Fi público .  
Seguridad en la nube.  
Uso de las redes sociales.

Seguridad en el hogar. Uso aceptable del equipo.  
Uso seguro del navegador.  
Protección de Datos. Bloqueo de pantalla. Entrenamiento dirigido. Informar incidentes.

```
bookdown::serve_book()
```

## 2 políticas para la estabilidad de los datos confidenciales

Se necesita que la organización tenga por escrito las políticas en ciberseguridad que regirán el trabajo diario, y que estas sean compartidas con todo el personal. Además de esto, es aconsejable reforzar el razonamiento de las políticas en ciberseguridad con la ayuda de debates a lo largo de el proceso de capacitación y a lo largo de el lapso de trabajo en la compañía.

política de protección de datos. política de contraseñas. política de actualizaciones. política de almacenamiento y copias de seguridad. política de seguridad en el puesto de trabajo. política de uso de correo electrónico. política de uso de wifi y redes externas. política de clasificación de la información.

### 2.1 Ataques de phishing

En el último año hemos visto un enorme aumento de los ataques de phishing. En particular, hubo una gran cantidad de correos electrónicos de phishing relacionados con la pandemia. El Grupo de Análisis de Amenazas de Google informó a mediados de abril de que había bloqueado 18 millones de correos electrónicos de malware y phishing con temática COVID-19 al día. Los ataques de phishing siguen siendo la causa más común de las violaciones de la ciberseguridad. Las cifras actuales reflejan claramente la necesidad de concienciación sobre los ataques de phishing, según las investigaciones el 91% de los ciberataques que tienen éxito son el resultado de una estafa de phishing.. Aunque las empresas son cada vez más conscientes del phishing, sigue siendo una amenaza creciente en 2021, en parte debido a la falta de concienciación de los empleados. Si se impulsa la formación en seguridad como parte de la filosofía de la empresa a través de una formación recurrente de concienciación en materia de seguridad, esta cifra puede reducirse drásticamente con el tiempo. El “spearphishing” es una forma de ataque más sofisticada y dirigida, que utiliza a trabajadores específicos de la empresa para dar legitimidad a un correo electrónico dirigido a un conjunto concreto de usuarios finales. Un correo electrónico en el que se suplanta al director general, por ejemplo, es probable que sea pulsado por la mayoría de los empleados, y podría contener un malware adjunto. La eficacia de este tipo de ataques ha dado lugar a nuevos y sofisticados desarrollos, como

el vishing y el smishing. Al formar a los usuarios finales para que reconozcan los correos electrónicos potencialmente dañinos y denuncien los sospechosos, esta amenaza puede reducirse considerablemente. Al ofrecer cursos de formación en ciberseguridad, la concienciación de los empleados sobre este tipo de ataques puede mejorarse enormemente con una formación constante. La simulación de ataques de phishing puede demostrar el riesgo potencial de estos ataques para la empresa.

## 2.2 Entrenamiento dirigido

Los tipos específicos de usuarios necesitan capacitación precisa para contrarrestar el spear phishing específico que puedan encontrar. El departamento de contabilidad, por ejemplo, necesita comprender por qué son un objetivo potencial. El CEO y otras personas con acceso privilegiado también necesitan comprender este tipo de ingeniería social específica. Y esto no puede ser una sesión de entrenamiento general para cubrir todo el phishing de lanza. Porque si los detalles de la situación parecen irrelevantes, es probable que tus alumnos se lo lleven. Los phishers de Spear están interesados en usar detalles personales y las tareas de proyectos en curso de una persona para calmar a una víctima para que abra correos electrónicos maliciosos y ejecute archivos adjuntos no autorizados. ¡Defiéndete de la misma manera! Use los mismos detalles que usaría un phisher de lanza para llegar a una víctima para crear su programa de entrenamiento. La capacitación dirigida incluye:

- Fraude de transferencias financieras para empleados capaces de transferir dinero
- El escepticismo necesario frente a las solicitudes del CEO de “emergencia” para los empleados que prestan servicios al CEO
- Capacitación contra restablecimientos de contraseñas fraudulentas para empleados que pueden restablecer contraseñas
- Entrenamiento contra credenciales de reingreso inesperadas después de leer el correo electrónico
- Entrenamiento estacional para diferentes épocas del año, como W-2 o fraude fiscal cerca de la temporada de impuestos

## 2.3 Seguridad en el hogar

Desafortunadamente, la amenaza de los actores maliciosos no desaparece cuando se abandona el lugar de trabajo. Muchas empresas permiten a sus empleados utilizar sus dispositivos personales, lo que supone un gran ahorro de costes y permite un trabajo flexible, sin embargo, existen riesgos asociados a ello. Las aplicaciones descargadas involuntariamente con malware en los dispositivos personales pueden poner en riesgo la integridad de la red de la empresa si, por ejemplo, se comprometen los datos de acceso. Además, la creciente red de recursos digitales a disposición de los trabajadores y las empresas ha aumentado la conectividad y la productividad. Sin embargo, estas aplicaciones también suponen un riesgo para el usuario: un estudio de Propeller descubrió que las campañas de phishing dirigidas a Dropbox tenían un porcentaje de clics del 13,6%. Aumentar

el conocimiento de los empleados, compartir archivos encriptados y autenticar las descargas reducirá el riesgo.

##Bloqueo de pantalla A menos que sean educados para ser conscientes de los riesgos, la mayoría de los usuarios de computadoras nunca pensaría en bloquear la pantalla de su computadora antes de alejarse de una computadora o dispositivo. Pero dejar una computadora a disposición de cualquiera puede dañar su identidad o compañía. En el extremo bajo de riesgo, un compañero de trabajo travieso podría enviar un correo electrónico de broma en su nombre. Pero cosas peores han sucedido. Las computadoras y dispositivos desbloqueados terminaron causando graves daños a la reputación de las compañías y usuarios inconscientes. Todos los usuarios necesitan que se les enseñe a bloquear la pantalla de su dispositivo cuando ya no estén cerca o en el control inmediato del dispositivo. Las mejores prácticas de bloqueo de pantalla incluyen:

- Los usuarios SIEMPRE deben bloquear su dispositivo al salir de la vecindad.
- Se debe solicitar a los usuarios que se autentiquen para desbloquear su dispositivo.
- Un dispositivo inactivo siempre debe bloquearse después de menos de 10 minutos.
- Un dispositivo bloqueado nunca debe revelar su contenido.

##Medios extraíbles Otro tema de concienciación sobre la seguridad que se utiliza a diario en las empresas son los medios extraíbles. Los medios extraíbles son aquellos soportes de almacenamiento portátiles que permiten a los usuarios copiar datos en el dispositivo y luego extraerlos del mismo para llevarlos a otro y viceversa. Los dispositivos USB que contienen malware pueden quedar a la vista de los usuarios finales cuando los conectan a su dispositivo. ” Unos investigadores dejaron caer casi 300 memorias USB en el campus de la Universidad de Illinois Urbana-Champaign. El 98% de estas unidades fueron recogidas. Además, el 45% de estas unidades no sólo fueron recogidas, sino que los individuos hicieron clic en los archivos que encontraron dentro ”.\* Además de conocer los riesgos, los empleados deben saber cómo utilizar estos dispositivos de forma segura y responsable en la empresa. Existen numerosas razones por las que una empresa puede decidir utilizar medios extraíbles en su entorno. Sin embargo, con todas las tecnologías, siempre habrá riesgos potenciales. Además de los propios dispositivos, es importante que los empleados protejan los datos que contienen. Ya sean personales o corporativos, todos los datos tienen algún tipo de valor. Algunos ejemplos comunes de medios extraíbles que tú y tus empleados podrás utilizar en el lugar de trabajo son:

- Memorias USB
- Tarjetas SD
- Los CD
- Teléfonos inteligentes

Este tema de concienciación sobre la seguridad debe incluirse en la formación y abarcar ejemplos de medios extraíbles, por qué se utilizan en las empresas, así como el modo en que los empleados pueden prevenir los riesgos, como la pérdida o el robo de dispositivos extraíbles, las infecciones por malware y la infracción de los derechos de autor.

##Contraseñas y autenticación Un elemento muy sencillo, pero que a menudo se pasa por alto, que puede ayudar a la seguridad de una empresa es la seguridad de las contraseñas. A menudo, las contraseñas más utilizadas serán adivinadas por actores maliciosos con la esperanza de obtener acceso a las cuentas. La

utilización de contraseñas sencillas o la existencia de patrones de contraseñas reconocibles para los empleados puede facilitar a los ciberdelincuentes el acceso a una gran variedad de cuentas. Una vez robada esta información, puede hacerse pública o venderse con fines lucrativos en la deep web. La implementación de contraseñas aleatorias puede dificultar mucho más el acceso de los actores maliciosos a una serie de cuentas. Otros pasos, como la autenticación de dos factores, proporcionan capas adicionales de seguridad que protegen la integridad de la cuenta. Su entrenamiento de mejores prácticas de contraseña debe incluir:

- Utilice la autenticación de dos factores (2FA) y la autenticación de múltiples factores (MFA) siempre que sea posible.
- Las contraseñas deben tener 8 caracteres o más.
- Las contraseñas no deberían ser tan comunes que se puedan violar en un instante. Por ejemplo, no use palabras como “contraseña” o “qwerty”.
- Use contraseñas únicas para cada sitio y servicio; no compartir entre sitios
- Cree y use cuidadosamente las “preguntas de restablecimiento” de la contraseña para asegurarse de que no contengan respuestas que sean fáciles de encontrar (como el apellido de soltera de su madre).

## #<sup>2</sup>Manejo de correo electrónico e internet

La mayoría de la malicia digital comienza con un correo electrónico no solicitado que contiene un archivo adjunto o un enlace malicioso, pidiéndole al destinatario que haga clic o se abra. Si su equipo está bien versado sobre cómo manejar adecuadamente los peligros inevitables del correo electrónico sin exponer a la compañía al riesgo, el correo electrónico no será su ruina. Por esta razón, el coaching por correo electrónico para todos los que usan una computadora de la empresa, o sus servidores, debería ser una parte clave de cualquier plan educativo para el usuario final. Las mejores prácticas de manejo de correo electrónico deben incluir:

- Entrene a la gente para que siempre sea un poco escéptico ante cualquier correo electrónico inesperado.
- Enseñe a todos a no hacer clic en un archivo adjunto que no esperaban. Llame al remitente primero para confirmar su origen.
- Nunca haga clic en ningún enlace de Internet inesperado sin verificar que el dominio URL sea legítimo.
- No habilite “contenido activo” en correos electrónicos de fuentes no confiables.
- Informe de correos electrónicos sospechosos a la seguridad de TI.
- Nunca haga clic en “Responder a todos” en grandes publicaciones de correo electrónico.

You can add parts to organize one or more book chapters together. Parts can be inserted at the top of an .Rmd file, before the first-level chapter heading in that same file.

Add a numbered part: # (PART) Act one {-} (followed by # A chapter)

Add an unnumbered part: # (PART\\*) Act one {-} (followed by # A chapter)

### **3 Medios extraíbles**

Otro tema de concienciación sobre la seguridad que se utiliza a diario en las empresas son los medios extraíbles. Los medios extraíbles son aquellos soportes de almacenamiento portátiles que permiten a los usuarios copiar datos en el dispositivo y luego extraerlos del mismo para llevarlos a otro y viceversa. Los dispositivos USB que contienen malware pueden quedar a la vista de los usuarios finales cuando los conectan a su dispositivo. ” Unos investigadores dejaron caer casi 300 memorias USB en el campus de la Universidad de Illinois Urbana-Champaign. El 98% de estas unidades fueron recogidas. Además, el 45% de estas unidades no sólo fueron recogidas, sino que los individuos hicieron clic en los archivos que encontraron dentro ”.\* Además de conocer los riesgos, los empleados deben saber cómo utilizar estos dispositivos de forma segura y responsable en la empresa. Existen numerosas razones por las que una empresa puede decidir utilizar medios extraíbles en su entorno. Sin embargo, con todas las tecnologías, siempre habrá riesgos potenciales. Además de los propios dispositivos, es importante que los empleados protejan los datos que contienen. Ya sean personales o corporativos, todos los datos tienen algún tipo de valor. Algunos ejemplos comunes de medios extraíbles que tú y tus empleados podréis utilizar en el lugar de trabajo son:

- Memorias USB
- Tarjetas SD
- Los CD
- Teléfonos inteligentes

Este tema de concienciación sobre la seguridad debe incluirse en la formación y abarcar ejemplos de medios extraíbles, por qué se utilizan en las empresas, así como el modo en que los empleados pueden prevenir los riesgos, como la pérdida o el robo de dispositivos extraíbles, las infecciones por malware y la infracción de los derechos de autor.

#### **3.1 Contraseñas y autenticación**

Un elemento muy sencillo, pero que a menudo se pasa por alto, que puede ayudar a la seguridad de una empresa es la seguridad de las contraseñas. A menudo, las contraseñas más utilizadas serán adivinadas por actores maliciosos con la esperanza de obtener acceso a las cuentas. La utilización de contraseñas sencillas o la existencia de patrones de contraseñas reconocibles para los empleados puede facilitar a los ciberdelincuentes el acceso a una gran variedad de cuentas. Una vez robada esta información, puede hacerse pública o venderse con fines lucrativos en la deep web. La implementación de contraseñas aleatorias puede dificultar mucho más el acceso de los actores maliciosos a una serie de cuentas. Otros pasos, como la autenticación de dos factores, proporcionan capas adicionales de seguridad que protegen la integridad de la cuenta. Su entrenamiento de mejores prácticas de contraseña debe incluir:

- Utilice la autenticación de dos factores (2FA) y la autenticación de múltiples factores (MFA) siempre que sea posible.
- Las contraseñas deben tener 8 caracteres o más.
- Las contraseñas no deberían ser tan comunes que se puedan violar en un instante. Por ejemplo, no use palabras como “contraseña” o “qwerty”.
- Use contraseñas únicas para cada sitio y servicio;
- no compartir entre sitios
- Cree y use cuidadosamente

las “preguntas de restablecimiento” de la contraseña para asegurarse de que no contengan respuestas que sean fáciles de encontrar (como el apellido de soltera de su madre).

### **3.2 Manejo de correo electrónico e internet**

La mayoría de la malicia digital comienza con un correo electrónico no solicitado que contiene un archivo adjunto o un enlace malicioso, pidiéndole al destinatario que haga clic o se abra. Si su equipo está bien versado sobre cómo manejar adecuadamente los peligros inevitables del correo electrónico sin exponer a la compañía al riesgo, el correo electrónico no será su ruina. Por esta razón, el coaching por correo electrónico para todos los que usan una computadora de la empresa, o sus servidores, debería ser una parte clave de cualquier plan educativo para el usuario final. Las mejores prácticas de manejo de correo electrónico deben incluir:

- Entrene a la gente para que siempre sea un poco escéptico ante cualquier correo electrónico inesperado.
- Enseñe a todos a no hacer clic en un archivo adjunto que no esperaban. Llame al remitente primero para confirmar su origen.
- Nunca haga clic en ningún enlace de Internet inesperado sin verificar que el dominio URL sea legítimo.
- No habilite “contenido activo” en correos electrónicos de fuentes no confiables.
- Informe de correos electrónicos sospechosos a la seguridad de TI.
- Nunca haga clic en “Responder a todos” en grandes publicaciones de correo electrónico.

## **4 Seguridad física**

Si eres alguien que deja sus contraseñas en notas adhesivas sobre su escritorio, es posible que quieras tirarlas. Aunque es probable que muchos ataques se produzcan a través de medios digitales, mantener los documentos físicos sensibles protegidos es vital para la integridad del sistema de seguridad de tu empresa. Ser consciente de los riesgos de dejar documentos, ordenadores desatendidos y contraseñas en la oficina o en casa puede reducir el riesgo de seguridad. Si se aplica una política en materia de ” escritorio despejado ”, puede reducirse significativamente la amenaza de que se roben o copien documentos desatendidos.

### **4.1 Seguridad de los dispositivos móviles**

La evolución del panorama de las tecnologías de la información ha mejorado la capacidad de los entornos de trabajo flexibles, y con ello los ataques a la seguridad más sofisticados. Dado que muchas personas tienen ahora la opción de trabajar sobre la marcha utilizando dispositivos móviles, este aumento de la conectividad ha traído consigo el riesgo de que se produzcan fallos de seguridad. Para las empresas más pequeñas, esto puede ser una forma eficaz de ahorrar presupuesto; sin embargo, la responsabilidad de los usuarios de los dispositivos es

un aspecto cada vez más relevante de la formación en 2021, especialmente para los trabajadores itinerantes o remotos. La llegada de aplicaciones móviles maliciosas ha aumentado el riesgo de que los teléfonos móviles contengan malware que podría conducir a una brecha de seguridad. Los cursos online de buenas prácticas para trabajadores con dispositivos móviles pueden ayudar a educar a los empleados para evitar riesgos, sin necesidad de protocolos de seguridad de alto coste. Los dispositivos móviles deben tener siempre la información sensible protegida por contraseña, encriptada o con autentificación biométrica en caso de pérdida o robo del dispositivo. El uso seguro de los dispositivos personales es una formación necesaria para cualquier empleado que trabaje con sus propios dispositivos. La mejor práctica comunitaria es asegurarse de que los trabajadores tengan que firmar una política en materia de seguridad móvil.

## **4.2 Trabajar a distancia**

En 2021, la necesidad obvia de trabajar a distancia, combinada con el aumento de su uso, llevó a muchas empresas a tomar medidas drásticas hacia sistemas de trabajo a tiempo completo desde casa. El trabajo a distancia puede ser positivo para las empresas y empoderar a los empleados promoviendo una mayor productividad y un mayor equilibrio entre la vida laboral y personal. Sin embargo, esta tendencia supone una mayor amenaza de violaciones de la seguridad si no se educa de forma segura sobre los riesgos del trabajo a distancia. Los dispositivos personales que se utilicen con fines laborales deben permanecer bloqueados cuando no estén vigilados y tener instalado un software antivirus. Si una empresa quiere ofrecer este incentivo, debería centrarse en educar a los empleados remotos sobre las prácticas de trabajo seguras.. Es probable que esta tendencia continúe en 2021/2022. Aunque esperamos ver la reapertura de oficinas y la vuelta a la vida laboral normal, las empresas han contratado cada vez más a trabajadores remotos, y es posible que los que se han adaptado al estilo de vida de teletrabajo prefieran trabajar de esta manera. La necesidad de formar a los empleados para que entiendan y gestionen su propia ciberseguridad es evidente. Como hemos visto, existe un panorama de amenazas cada vez más amplio dirigido a estas personas. Garantizar que tengan la seguridad en mente es un tema clave para 2021.

## **4.3 Wi-Fi público**

Algunos empleados que necesitan trabajar a distancia, viajar en tren y trabajar sobre la marcha pueden necesitar una formación adicional para saber cómo utilizar de forma segura los servicios de Wi-Fi públicos. Las redes Wi-Fi públicas falsas, que a menudo se hacen pasar por Wi-Fi gratuito en las cafeterías, pueden dejar a los usuarios finales en situación de vulnerabilidad al introducir información en servidores públicos no seguros. La educación de los usuarios sobre el uso seguro de las redes Wi-Fi públicas y las señales comunes para detectar

una posible estafa aumentará la concienciación de las empresas y minimizará el riesgo. La revista WIRED ofrece una guía útil para evitar los riesgos del Wi-Fi público.

## 5 Seguridad en la nube

La computación en la nube ha revolucionado las empresas y la forma de almacenar y acceder a los datos. Estas aplicaciones digitales están transformando las empresas, pero el hecho de que grandes cantidades de datos privados se almacenen de forma remota conlleva el riesgo de que se produzcan hackeos a gran escala. Muchas grandes empresas están trabajando en la protección de datos, pero si se elige el proveedor de servicios en la nube adecuado, el almacenamiento en la nube puede ser una forma mucho más segura y rentable de almacenar los datos de la empresa. Al igual que en los otros temas mencionados, la piratería interna es una amenaza mucho mayor que para las empresas de la nube a gran escala. Gartner predice que para el próximo año, el 99% de los incidentes de seguridad en la nube serán culpa del usuario final. Por lo tanto, la formación en ciberseguridad puede ayudar a guiar a los empleados en el uso seguro de las aplicaciones basadas en la nube.

### 5.1 Uso aceptable del equipo

- Los dispositivos comerciales son propiedad exclusiva de la empresa. Solo el negocio puede asignar, eliminar y determinar el control sobre esos dispositivos.
  - No hay expectativas de privacidad cuando se utiliza un dispositivo de propiedad empresarial. La compañía puede leer los correos electrónicos de los empleados u otras comunicaciones a su propia discreción, sin previo aviso.
  - No se permiten actividades ilegales o poco éticas en dispositivos comerciales.
  - La empresa puede deshabilitar o restablecer cualquier contraseña creada por el usuario sin previo aviso.
  - El uso personal está permitido siempre que no sea excesivo (según lo determine la empresa) y no viole una de las pautas anteriores.
  - El incumplimiento de este acuerdo de uso aceptable puede dar lugar a acciones adversas, incluida la eliminación del mismo dispositivo de la compañía y hasta la terminación.
- ##Uso de las redes sociales Todos compartimos gran parte de nuestras vidas en las redes sociales: desde las vacaciones hasta los eventos y el trabajo. Pero compartir en exceso puede hacer que la información sensible esté disponible, lo que facilita que un actor malicioso se haga pasar por una fuente de confianza (consulta: la ingeniería social). Educar a los empleados en la protección de la configuración de privacidad de sus cuentas de redes sociales y evitar la difusión de información pública de su empresa reducirá el riesgo de la ventaja potencial que los hackers pueden obtener de este acceso a la red personal.

## **5.2 Uso seguro del navegador**

Usar un navegador para navegar por Internet es una actividad de alto riesgo. Todos los miembros de su empresa deben aprender a navegar de forma inteligente y segura por Internet sin ejecutar archivos o contenido malicioso. Las mejores prácticas de navegación en Internet deben incluir:

- Instrucciones para garantizar que su navegador esté completamente parcheado contra vulnerabilidades de seguridad críticas.
- Advertencias contra la instalación de complementos innecesarios sin la aprobación del administrador.
- Precauciones contra la navegación por Internet con una cuenta altamente privilegiada (por ejemplo, la del administrador).
- Advertencias de no ejecutar ejecutables inesperados presentados en un navegador.
- Capacitación sobre cómo verificar la legitimidad de los dominios URL. Pautas sobre qué hacer al encontrar instrucciones en línea que le indican que evite, o cómo evitar, las advertencias de seguridad.

## **5.3 Protección de Datos**

La importancia de la protección de datos se ha enfocado con las nuevas leyes y regulaciones de privacidad y protección de datos como el GDPR de Europa y la Ley de Privacidad del Consumidor de California (CCPA). Además de asegurarse de que los datos que recopila son necesarios y se recopilan y utilizan legalmente, su capacitación en protección de datos también debe cubrir estos temas importantes:

- Una definición de qué tipo de información necesita ser protegida, con ejemplos.
- Cómo deshacerse de los datos cuando ya no se necesitan.
- La necesidad de cifrar todos los datos confidenciales cuando están en reposo y durante las comunicaciones de red.
- La necesidad de etiquetar los datos de acuerdo con su sensibilidad o criticidad (por ejemplo, alto secreto, secreto, confidencial, público, etc.)
- Protocolos y la documentación requerida para compartir datos.
- La importancia de hacer una copia de seguridad de los datos críticos, encriptados y protegidos con contraseña, en dos o más lugares.
- Aliente al personal a discutir estos problemas con su oficial de protección de datos cuando tenga alguna duda.

## **6 Informar incidentes**

El tiempo promedio que le toma a una empresa descubrir un evento de piratería maliciosa es de 8 meses, e incluso entonces es descubierto por alguien externo a la empresa de la víctima. Lamentablemente, muchas veces el incidente de seguridad fue notado por alguien dentro de la empresa mucho tiempo antes de que el equipo oficial de respuesta al incidente se enterara. El mantra, “Si ves algo, di algo” se aplica tanto en el mundo digital como en el mundo real. Todos los empleados deben saber cómo reconocer e informar incidentes de seguridad. Desea crear una cultura en la que las personas no tengan miedo de informar

algo que no parece correcto. Deben ser alentados a informar todos los eventos sospechosos sin temor ni repercusiones. Use más “zanahorias” y menos “palos”. Las recomendaciones comunes de informes de incidentes incluyen:

- Algunos ejemplos memorables de incidentes de seguridad comunes.
- ¿A quién llamas si ves algo sospechoso?
- Pautas sobre cómo informar un incidente de seguridad.
- Lo que la gente debería esperar después de haber realizado un informe.
- Mucho aliento amistoso destinado a convencer a las personas para que denuncien proactivamente los incidentes de seguridad.
- Qué hacer con una computadora o dispositivo que un empleado cree que puede haber sido comprometido. (¿Apagarlo? ¿Desmantelarlo? ¿Llevarlo al departamento de TI?)