Lista de comprobación de la seguridad de los datos en la incorporación de nuevos empleados

¿Ha dado recientemente la bienvenida a su organización a nuevos empleados? Si es así, es fundamental abordar la seguridad de la información desde el principio de su trabajo. Los errores o descuidos de los empleados son una de las principales causas de las violaciones de datos, y una orientación exhaustiva puede contribuir en gran medida a mitigar el riesgo. Los gerentes y los equipos de liderazgo pueden ayudar a construir y reforzar la cultura de seguridad total de una empresa, esbozando estrategias y asegurándose de que los empleados reconocen su papel en el mantenimiento de la seguridad de los datos.

¿LO SABÍA?

Casi la mitad (49%) de los líderes empresariales encuestados indican que la falta de comprensión de las amenazas y riesgos para la organización es el mayor obstáculo para que los empleados sigan las políticas de seguridad de la información.1

A continuación se presenta una lista de comprobación de temas de seguridad de la información, tanto electrónicos como en papel, para revisar durante la incorporación de nuevos empleados.

- ☐ **Normas de seguridad de la información.**
  Las violaciones de datos pueden dar lugar a multas y dañar la reputación de una empresa. Familiarizar a los empleados con los aspectos clave de las leyes de seguridad de datos relevantes puede proporcionar un contexto valioso para las discusiones importantes sobre seguridad de datos.

- ☐ **Notificación de incidentes.**
  A pesar de los esfuerzos de una empresa, puede producirse una fuga y violación de datos. Los empleados deben saber cuándo y cómo denunciar estos hechos y tener la seguridad de que no serán sancionados por hablar. Asegúrese de informar a sus nuevos empleados de las percepciones y expectativas sobre la notificación de incidentes desde el principio, para que tanto los nuevos como los actuales empleados entiendan cómo reaccionar si se produce una violación de datos.

- ☐ **Procedimientos de impresión.**
  Los errores más comunes, como dejar inadvertidamente documentos confidenciales al aire libre en lugares como las impresoras, aumentan el riesgo de filtración de datos. Es vital reforzar la importancia de recuperar rápidamente los materiales impresos de la impresora, ya que esto puede reducir la probabilidad de robo de información. Si su empresa protege sus impresoras con contraseñas, no olvide instruir a los nuevos empleados sobre cómo acceder y preservar la seguridad de esas contraseñas.

- ☐ **Políticas de dispositivos electrónicos.**
  Los teléfonos móviles y las tabletas personales en el lugar de trabajo son cómodos, pero pueden suponer un mayor riesgo de incidentes de seguridad. Al incorporar a los nuevos empleados, asegúrese de que entienden cómo proteger sus dispositivos en todo momento.

Fuente: 1 Informe sobre protección de datos de Shred-it, 2021

Protegemos lo que importa.

Shred-it®
Una Solución Stericycle®

LISTA DE COMPROBACIÓN DE LA SEGURIDAD DE LOS DATOS EN LA INCORPORACIÓN DE NUEVOS EMPLEADOS

☐ Mantener un escritorio limpio.

Si su empresa cuenta con una política de mesas limpias, debe explicar exactamente lo que significa para los nuevos empleados. Normalmente, esto requiere que los empleados guarden bajo llave todos los documentos que muestren información confidencial; retiren los documentos no esenciales de la parte superior de las mesas y activen la pantalla de bloqueo del ordenador antes de salir por un tiempo prolongado o al final del día.

☐ Protocolos de contraseña.

Las contraseñas son una precaución de seguridad esencial. Los nuevos empleados deben estar completamente informados sobre la política de contraseñas de su organización y saber lo que significa crear contraseñas seguras. Una buena contraseña incorpora letras mayúsculas y minúsculas, números y símbolos, y debe actualizarse regularmente. Si su empresa tiene un programa obligatorio de actualización de contraseñas, asegúrese de que los nuevos empleados estén al tanto.

☐ Eliminación integral de documentos.

Los nuevos empleados deben saber cómo deshacerse correctamente de los documentos de su empresa. Informar a los nuevos empleados de los procedimientos de eliminación de documentos existentes puede ayudar a mitigar los riesgos y limitar las complicaciones de la protección de datos. Tal vez sea mejor introducir una política Shred-it All/Destrucción total y aconsejarles que se deshagan de todos los documentos en una consola segura para garantizar una destrucción segura. Esto eliminará las conjeturas sobre lo que puede ser confidencial o no. Esto no sólo contribuye a la seguridad de los documentos confidenciales, sino que, dado que todo el papel triturado se recicla, también es una buena práctica en términos de sostenibilidad.

☐ Precauciones con el correo electrónico.

Los incidentes de seguridad cibernética a menudo ocurren porque los empleados hacen clic en correos electrónicos que no deberían. Los nuevos empleados deben recibir capacitación sobre cómo reconocer correos electrónicos sospechosos, incluidos malware, esquemas de phishing y ransomware, para que puedan aprender a evitar situaciones de riesgo.

Para saber más sobre las mejores prácticas de seguridad de la información, visite shredit.es o llame al 900 170 500

Protegemos lo que importa.

Shred-it®
Una Solución Stericycle®