Elemento/Política	¿Cómo se va a verificar?	¿Qué es un fallo?	¿Qué es un acierto?	Check
Conocimiento de la normativa de protección del puesto de trabajo	Se enviará un formulario de Google a los empleados a través del correo electrónico con preguntas específicas sobre la normativa de protección del puesto de trabajo y medidas de seguridad.	El empleado responde mal en más de un 35% de las preguntas.	El empleado acierta un 65% o más de las preguntas.	☑
Uso de contraseñas seguras	Revisión de contraseñas de los dispositivos.	Contraseñas débiles, compartidas o almacenadas de manera insegura.	Contraseñas fuertes y almacenadas de manera segura.	☑
Actualización del sistema operativo	Verificación de la versión del sistema operativo en uso.	El sistema operativo no está actualizado con las últimas versiones o parches de seguridad.	El sistema operativo está actualizado con las últimas versiones y parches de seguridad.	☑
Uso de software de seguridad	Comprobar la presencia y actualización de software antivirus y cortafuegos.	Falta de software de seguridad o software desactualizado.	Software de seguridad instalado y actualizado.	☐
Copias de seguridad regulares	Comprobar si se realizan copias de seguridad de los datos importantes.	No se realizan copias de seguridad o son poco frecuentes.	Copias de seguridad regulares de datos importantes.	☐
Protección de la información confidencial	Revisión de acceso a datos sensibles.	Acceso no autorizado a información confidencial.	Restricciones de acceso adecuadas a datos sensibles.	☑
Uso de conexiones seguras	Verificar si se utilizan conexiones seguras (por ejemplo, VPN) para acceder a recursos corporativos.	Conexiones no seguras o no autorizadas.	Uso de conexiones seguras para acceder a recursos corporativos.	☑
Política de uso aceptable de dispositivos	Revisión de políticas y acuerdos de uso aceptable de dispositivos.	Incumplimiento de las políticas de uso aceptable.	Cumplimiento de las políticas de uso aceptable.	☐
Actualización de software y de aplicaciones	Comprobar la actualización de software y aplicaciones instalados en los portátiles.	Software o aplicaciones desactualizados y vulnerables.	Software y aplicaciones actualizados regularmente.	☑
Formación en ciberseguridad	Evaluación trimestral a través de cuestionarios interactivos y participación en simulacros de phishing.	El empleado no demuestra comprensión de las amenazas comunes y mejores prácticas de seguridad.	El empleado demuestra comprensión de las amenazas comunes y mejores prácticas de seguridad.	☑
Gestión de vulnerabilidades	Análisis de escaneos de seguridad, evaluación de riesgos y aplicación de correcciones	Existencia de vulnerabilidades sin abordar en sistemas y aplicaciones.	Asignación precisa de permisos de acceso según roles y responsabilidades.	☑
Gestión de identidades y accesos	Revisión de los permisos de acceso, con énfasis en la concordancia entre los roles y responsabilidades de los empleados y sus privilegios de acceso.	Asignación incorrecta de permisos de acceso que no se ajustan a roles y responsabilidades.	Software y aplicaciones actualizados regularmente.	☑
Supervisión y detección de amenazas	Revisión continua de registros y eventos de seguridad para identificar comportamientos inusuales o actividades maliciosas.	Conexiones no seguras o no autorizadas.	Supervisión y detección efectivas de comportamientos inusuales o actividades maliciosas.	☑
Gestión de incidentes de seguridad	Simulacros de incidentes de seguridad y evaluación de la eficacia del procedimiento de respuesta.	Respuesta ineficaz o falta de procedimientos de gestión de incidentes.	Respuesta eficaz y procedimientos de gestión de incidentes bien establecidos.	☐
Auditorías y evaluaciones regulares	Auditorías y evaluaciones de seguridad de la información e infraestructura tecnológica para garantizar el cumplimiento de políticas y estándares.	Incumplimiento significativo de políticas y estándares de seguridad.	Cumplimiento adecuado de políticas y estándares de seguridad.	☑
Educación continua en ciberseguridad	Entrega de material educativo y actualizaciones sobre nuevas amenazas y mejores prácticas de seguridad.	Falta de participación o interés continuo en la educación en ciberseguridad.	Participación activa y muestra de interés continuo en la educación en ciberseguridad.	☑
Política de copias de seguridad y recuperación	Evaluación de la implementación de la política de copias de seguridad y restauración de datos críticos.	Falta de coherencia en la aplicación de la política de copias de seguridad y recuperación.	Aplicación coherente de la política de copias de seguridad y recuperación.	☑
Evaluación de terceros	Revisión de medidas de seguridad implementadas por proveedores y terceros.	No cumplen con los estándares de seguridad establecidos por la empresa	Verificación de que el proveedor sigue prácticas de seguridad robustas y mantiene un nivel adecuado de protección de la información confidencial.	☑