Auditoría Digital de Ciberseguridad

Empresa: Onlychollos
Número de empleados: Yo solo/a
Sector: Hostelería y turismo
Solicita la auditoría: Milayton
Cargo: jefe

ÍNDICE

1. RESUMEN EJECUTIVO
2. EVALUACIÓN DE DISPOSITIVOS Y SOFTWARE
3. ANÁLISIS DE HÁBITOS DIGITALES
4. GESTIÓN DE CONTRASEÑAS Y ACCESOS
5. FORMACIÓN Y PLAN DE MEJORA
6. EVALUACIÓN
7. CIERRE

1. RESUMEN EJECUTIVO

Este informe es una fotografía general del nivel de ciberseguridad de Onlychollos basado en las respuestas que habéis proporcionado en la auditoría digital. El objetivo es que tengáis una visión clara de los puntos fuertes y de las áreas de mejora, expresado en un lenguaje sencillo y orientado al negocio. La ciberseguridad no es solo un tema técnico: está directamente relacionada con la continuidad de vuestro trabajo, la confianza de los clientes y el cumplimiento legal.

En las siguientes páginas vais a encontrar un análisis por bloques que os ayudará a entender dónde estáis hoy y qué pasos dar para estar mejor protegidos mañana.

La auditoría de ciberseguridad realizada a Onlychollos revela un panorama mixto en cuanto a su protección digital. Por un lado, se identifican buenas prácticas en la gestión de accesos y actualizaciones regulares de software, lo que evidencia un compromiso con la seguridad básica y mantenimiento actualizado de sus sistemas. Sin embargo, persisten vulnerabilidades que requieren atención inmediata, como la ausencia de controles robustos en la protección de datos sensibles y la falta de protocolos claros para la respuesta ante incidentes de seguridad.

Además, se observa que la empresa podría mejorar la formación y concienciación del personal en temas de ciberseguridad, ya que algunos riesgos asociados a errores humanos podrían ser mitigados con capacitación adecuada. En general, Onlychollos muestra un esfuerzo inicial en proteger sus activos digitales, pero debe fortalecer sus defensas y formalizar políticas internas para asegurar una protección integral y minimizar posibles amenazas en el futuro.

2. EVALUACIÓN DE DISPOSITIVOS Y SOFTWARE

Los ordenadores, móviles y programas son la base de la operativa diaria: gestión de pedidos, facturación o atención al cliente. Si estos activos no están bien cuidados, cualquier problema técnico puede convertirse en un freno para la productividad y una puerta abierta a riesgos mayores.
En este bloque revisamos cómo estáis gestionando esa base tecnológica.

[B]Estado de los sistemas operativos[/B]: El cliente utiliza sistemas operativos basados en Linux, tales como Ubuntu, Fedora y Debian. Sin embargo, la actualización de estos sistemas se realiza manualmente y, en la práctica, no se actualizan nunca en algunos casos, mientras que sólo algunos dispositivos reciben actualizaciones. Esto implica un [B]riesgo significativo de vulnerabilidades críticas[/B], ya que la falta de actualizaciones expone a los sistemas a posibles ataques y brechas de seguridad.

[B]Aspecto de las licencias de software[/B]: No se menciona la existencia de licencias oficiales para el software en uso, lo que impide evaluar su legalidad y actualización. Se recomienda realizar un inventario y validar las licencias para asegurar la conformidad y acceso a soporte.

[B]Política de copias de seguridad[/B]: No se realizan copias de seguridad en ninguno de los dispositivos, lo que representa un [B]riesgo crítico ante posibles incidentes de pérdida de datos[/B], fallos de hardware o ataques de malware. Es imprescindible implementar una estrategia de backups periódicos, preferiblemente automatizada y con almacenamientos externos.

[B]Protección antivirus[/B]: La protección actual se limita a un antivirus gratuito, cuya capacidad para detectar amenazas avanzadas puede ser limitada. No se cuenta con soluciones antivirus para todos los sistemas. Se recomienda evaluar la implementación de [B]medidas de seguridad antivirus más robustas[/B] y complementarlas con otras herramientas de protección.

[B]Antecedentes de incidentes[/B]: No se han reportado incidentes previos, pero dadas las condiciones mencionadas —actualizaciones irregulares o inexistentes, ausencia de backups y limitada protección antivirus— existe un [B]alto riesgo potencial de incidentes de seguridad[/B], incluyendo ataques de malware, ransomware o pérdida de datos. Se recomienda establecer un plan de respuesta y monitoreo para reducir dicha exposición.

3. ANÁLISIS DE HÁBITOS DIGITALES

El día a día digital —abrir correos, navegar por internet o conectarse a una red— parece rutinario, pero es el punto de entrada más común para ataques contra pymes. Muchas veces no se trata de tecnología, sino de cómo las personas interactúan con ella.
Este bloque refleja cómo vuestros hábitos influyen en la seguridad de la empresa.

Los hábitos digitales mostrados por la empresa presentan varios puntos de preocupación. El acceso "desde cualquier sitio" sin especificar medidas de seguridad expone a riesgos críticos, especialmente si no se utilizan conexiones seguras como VPN o autenticación multifactor. Esto puede facilitar el acceso no autorizado y la interceptación de datos sensibles.

Es positivo que solo se descarguen archivos o se haga clic en enlaces provenientes de remitentes conocidos, ya que este comportamiento reduce la probabilidad de infección por malware o ataques de phishing, dos tipos de amenazas frecuentes en entornos corporativos. Sin embargo, el desconocimiento sobre el uso de extensiones de seguridad puede ser una vulnerabilidad si no se están implementando herramientas que protejan el navegador o el correo electrónico.

El hecho de que nunca se acceda de forma remota genera cierta contradicción con el comentario de que sí se utiliza Outlook 2016 o 365 "tanto fuera como dentro de la empresa". Esto sugiere que podría haber accesos remotos no controlados o sin protocolos de seguridad robustos, lo cual aumenta la exposición a posibles brechas.

No se utilizan dispositivos USB y no se permite acceso remoto, lo cual es positivo para minimizar vectores de ataque comunes. Sin embargo, la respuesta "no lo sé" frente a ciertas medidas indica falta de capacitación o comunicación interna sobre políticas de ciberseguridad, lo que es un riesgo importante, pues la seguridad digital depende en gran medida del conocimiento y comportamiento de los empleados.

Se recomienda implementar controles más estrictos para el acceso remoto, incluyendo el uso obligatorio de VPN y autenticación fuerte. Además, debe exigirse la adopción de extensiones de seguridad y antivirus actualizados en todas las estaciones, junto con programas de formación continua para aclarar dudas y reforzar prácticas responsables. Así la empresa podrá reducir significativamente su nivel de exposición a amenazas digitales.

4. GESTIÓN DE CONTRASEÑAS Y ACCESOS

Las contraseñas son las llaves de acceso a la información y a los sistemas. Si estas llaves no están bien gestionadas, cualquiera podría entrar en la 'casa digital' de la empresa.

Aquí analizamos cómo controláis el acceso y qué medidas adicionales ayudan a reforzar la protección.

La empresa no utiliza un gestor de contraseñas, lo que representa una vulnerabilidad significativa en la gestión de credenciales. Al no contar con una herramienta centralizada y segura, se incrementa el riesgo de que las contraseñas sean almacenadas de manera insegura, como en documentos no protegidos o notas físicas, facilitando el acceso no autorizado a sistemas internos.

Además, al desconocer si cuentan con una política o herramienta para la revisión periódica de contraseñas, la empresa se expone a amenazas críticas derivadas del uso prolongado de claves posiblemente comprometidas. La falta de rotación y auditoría dificulta la detección de accesos indebidos y reduce la capacidad de respuesta ante incidentes de seguridad.

Aunque existe conocimiento de que algunas contraseñas son fuertes, la no

compartición de contraseñas no está garantizada, ya que la ausencia de un responsable designado para la gestión de accesos puede generar prácticas informales de compartición entre empleados. Esta situación aumenta el riesgo de fuga de credenciales y dificulta la trazabilidad de acciones en los sistemas.

La inexistencia de autenticación en dos pasos (2FA) es una carencia crítica que expone a la organización a ataques de suplantación de identidad y acceso no autorizado, incluso si las contraseñas son complejas. Implementar [B]2FA[/B] es una medida de seguridad altamente recomendada para proteger cuentas y datos sensibles, incrementando considerablemente la seguridad del entorno digital.

Se recomienda a la empresa implementar un gestor de contraseñas robusto que permita almacenar y compartir credenciales de manera segura y cifrada, además de establecer políticas claras para la creación, cambio y revisión periódica de contraseñas. La designación de un responsable de gestión de accesos facilitará la supervisión y control de las prácticas de seguridad. Finalmente, integrar la [B]autenticación en dos fases[/B] debe ser una prioridad para fortalecer la protección contra amenazas comunes en entornos corporativos.

5. FORMACIÓN Y PLAN DE MEJORA

La ciberseguridad no depende solo de la tecnología, también de las personas y de cómo reaccionan. Un empleado formado puede detectar un engaño antes de que cause daño. Y si ocurre un incidente, tener un plan de actuación es lo que marca la diferencia entre resolverlo rápido o sufrir pérdidas importantes.
Este bloque revisa vuestra preparación en ambos aspectos.

Juan S.A. ha apostado por la formación interna de su equipo en materia de ciberseguridad, lo que denota una intención positiva de cultivar una cultura organizacional consciente de las amenazas digitales. Esta formación, al ser interna, puede resultar más personalizada y ajustada a las necesidades específicas de la empresa, facilitando un mejor entendimiento de los riesgos particulares del sector en que opera.

Sin embargo, la ausencia de un plan de respuesta ante incidentes plantea un riesgo crítico para la continuidad operativa y la gestión eficaz de ciberataques o brechas de seguridad. No contar con un documento estructurado que guíe las acciones en caso de una incidencia limita la capacidad de reacción inmediata, puede provocar pérdidas significativas de datos, daños reputacionales severos y costos económicos considerables. Esta falta de preparación formal es una vulnerabilidad que expone a la empresa a graves consecuencias ante cualquier eventualidad tecnológica.

La formación interna recibida podría estar limitando su alcance si no incluye temáticas esenciales como la identificación de amenazas, la gestión de crisis, procedimientos de escalado, y prácticas de recuperación. Sin un plan de respuesta, la preparación teórica no se traduce en capacidad real de acción bajo presión, afectando directamente la resiliencia digital de la organización. Esto también pone en evidencia una brecha entre la capacitación y la aplicación práctica en escenarios críticos.

Es importante recomendar que, junto con la formación continua, se desarrolle y documente un plan robusto de respuesta ante incidentes que incluya roles, responsabilidades, protocolos paso a paso y ejercicios de simulación periódicos. Esto permitirá transformar la cultura de ciberseguridad en una estrategia activa y dinámica, reduciendo el impacto de ataques y facilitando la recuperación rápida. Además, se recomienda considerar complementar la formación interna con recursos externos especializados que aporten perspectivas actualizadas y mejores prácticas del sector.

El hecho de contar con formación interna es una buena práctica que permite involucrar directamente al personal y fomentar una conciencia colectiva sobre seguridad. Este enfoque beneficia a la empresa al generar un equipo más atento y preparado para detectar anomalías antes de que escalen. Sin embargo, para maximizar estos beneficios es fundamental integrar esta capacitación con un plan formal de respuesta, evitando que el conocimiento quede sólo en teoría y garantizando una gestión eficaz ante incidentes reales.

6. EVALUACIÓN

En este apartado resumimos los principales riesgos y fortalezas detectados en vuestra empresa. No se trata de un examen ni de una nota final, sino de una guía visual para que podáis priorizar esfuerzos.
Los riesgos se clasifican en críticos, moderados y leves, en función de su impacto en el negocio. Las fortalezas muestran lo que ya estáis haciendo bien y que conviene mantener en el tiempo.

A continuación, se listan las vulnerabilidades y fortalezas detectadas en Onlychollos

[B]VULNERABILIDADES CRÍTICAS[/B]

- Falta de actualizaciones regulares en sistemas operativos basados en Linux, dejando expuestos los sistemas a vulnerabilidades críticas.
- Ausencia de copias de seguridad en todos los dispositivos, lo que implica un riesgo crítico ante pérdidas de datos, fallos o ataques de malware.
- No existencia de un plan de respuesta ante incidentes, lo que limita la capacidad de reacción y gestión efectiva frente a ciberataques o brechas de seguridad.
- Inexistencia de autenticación en dos pasos (2FA), incrementando el riesgo de accesos no autorizados y suplantación de identidad.
- Falta de un gestor de contraseñas para una gestión segura y centralizada de credenciales, junto con déficit en políticas de creación y rotación de contraseñas.
- Acceso remoto sin controles estrictos ni protocolos robustos (ausencia confirmada de VPN obligatoria y autenticación fuerte), elevando el riesgo de accesos no autorizados y exposición de datos sensibles.

[B]VULNERABILIDADES MODERADAS[/B]
- Uso de protección antivirus limitada a soluciones gratuitas y no generalizadas en todos los sistemas, lo que reduce la efectividad frente a amenazas avanzadas.
- Desconocimiento y falta de implementación de extensiones o herramientas de seguridad para navegador y correo electrónico, potencialmente vulnerables a ataques de phishing o malware.
- Posible incumplimiento en la legalidad y soporte de software por ausencia de inventario y validación de licencias oficiales.
- Falta de un responsable designado para la gestión de accesos y supervisión en la compartición de contraseñas, aumentando riesgos y dificultando trazabilidad de acciones.
- Capacitación interna en ciberseguridad no complementada con conocimientos específicos sobre gestión práctica de incidentes, crisis y recuperación.

[B]VULNERABILIDADES LEVES[/B]
- Indefinición y falta de comunicación clara sobre medidas de seguridad relacionadas con los hábitos digitales del personal (respuesta "no lo sé" sobre ciertos controles).
- Contradicciones detectadas entre afirmaciones sobre accesos remotos y la no autorización documental de los mismos, evidenciando falta de claridad en políticas y controles internos.

[B]FORTALEZAS DETECTADAS[/B]
- Uso de sistemas operativos Linux, que poseen una arquitectura generalmente robusta frente a amenazas comunes.
- Conductas positivas del equipo, como descargar archivos y abrir enlaces solo de remitentes conocidos, reduciendo el riesgo de infecciones por malware y ataques

de phishing.
- No uso de dispositivos USB ni permiso para acceso remoto, lo que disminuye vectores habituales de ataque.
- Inversión en formación interna en materia de ciberseguridad, promoviendo una cultura organizacional consciente y adecuada a las necesidades específicas de la empresa.

7. CIERRE

Este diagnóstico es un primer paso. Te ha ofrecido una idea clara del nivel actual de Onlychollos en materia de ciberseguridad y de las principales áreas que requieren atención. Se trata de un análisis basado en las respuestas que habéis proporcionado, no en pruebas técnicas directas sobre los sistemas de la empresa. Para tener una visión completa, recomendamos realizar una Auditoría Interna y Externa de Ciberseguridad, en la que nuestros especialistas revisarán en detalle vuestros equipos y configuraciones. Así obtendréis un plan adaptado a vuestra realidad, con medidas concretas, priorizadas y acompañamiento en su implementación.

NOTA DE TRANSPARENCIA: Este informe ha sido elaborado con el apoyo de tecnologías de Inteligencia Artificial, integradas en un proceso diseñado y supervisado por profesionales especializados en ciberseguridad. El objetivo de este diagnóstico es ofrecer a la empresa una primera visión clara y accionable sobre su nivel de protección digital, con recomendaciones prácticas que aportan valor inmediato.

La Inteligencia Artificial nos permite generar este análisis de forma personalizada y de manera automática, pero es el equipo de expertos de Cosmomedia quien ha definido la metodología, los criterios de evaluación y las recomendaciones que lo sustentan. De este modo, aseguramos que cada informe sea una herramienta útil para tomar decisiones y un punto de partida sólido hacia una auditoría completa y una estrategia de ciberseguridad adaptada a la realidad de cada negocio.