Estimado Cliente,

Como parte de nuestro compromiso por mejorar el nivel de ciberseguridad de las organizaciones, hemos analizado la información que nos proporcionó y, en consecuencia, los distintos aspectos críticos que conforman su infraestructura, procesos y políticas de protección digital.

Tras la evaluación realizada, detectamos que el nivel actual de madurez en ciberseguridad de su compañía es un nivel intermedio.
Las organizaciones en esta etapa suelen presentar un enfoque intermedio respecto a la ciberseguridad, con tecnologías específicas de protección y procesos formalizados que les permiten mitigar ciertos tipos de riesgos y amenazas, así como también responder de forma reactiva ante los incidentes.

Las tecnologías y procesos habituales son:

Plataforma de protección para endpoints y/o EDR básico.

Firewall implementado con controles capa 7 y soluciones específicas de protección para email.

Campañas de concientización esporádicas y entrenamientos puntuales en ciberseguridad.

Ciertos procesos formales definidos y formalizados (altas y bajas de usuarios, políticas de contraseñas, backups regulares, etc.).

Si bien existe una mayor consciencia sobre la importancia de la seguridad de la información y protección de los activos, aún presenta áreas de mejora que podrían evitar y reducir incidentes que deriven en pérdida de datos sensibles, interrupciones operativas o daños a la reputación institucional.

Entre los hallazgos más relevantes dentro de este tipo de organizaciones, destacamos:

- Ciberseguridad considerada relevante por el área de TI, pero aún no plenamente integrada en la agenda del management.
- Conciencia moderada sobre los riesgos existentes y limitaciones para abordarlos de manera proactiva.
- No hay evaluación continua de riesgos ni pruebas de penetración regulares.
- Equipo dedicado de TI con al menos un especialista dedicado a ciberseguridad.
- Presupuesto asignado para TI con un porcentaje específico (aunque limitado) para seguridad
- Respuesta ante incidentes predominantemente reactiva.
- Cumplimiento parcial de normativas o estándares de la industria.
- Falta de visibilidad completa sobre todos los dispositivos, usuarios y accesos.

Para evolucionar desde este nivel intermedio, las organizaciones deben adoptar un enfoque más estratégico y estructurado. Esto implica implementar un modelo de madurez reconocido, que les permita evaluar su situación de forma integral. También resulta fundamental diseñar e implementar un plan de respuesta ante incidentes, e incorporar soluciones proactivas de detección y respuesta, junto con auditorías periódicas y evaluaciones de vulnerabilidades.

Fomentar una cultura de seguridad desde los niveles directivos y alinear las iniciativas de ciberseguridad con los objetivos del negocio, son pasos clave para una gestión eficaz y continua del riesgo.

Entendemos que esta situación puede ser preocupante, pero también representa una oportunidad para establecer las bases de una estrategia integral de ciberseguridad.

Desde Kaspersky, estamos convencidos que podemos acompañarlo en el diseño e implementación de un plan a medida que le permita mitigar y reducir riesgos, así como también fortalecer su organización frente a las amenazas actuales.

¿Cómo podemos ayudarlo?

Contamos con un porfolio de soluciones y servicios pensados para acompañar cada etapa de desarrollo de su compañía.

NEXT EDR Optimum:

Plataforma completa de protección para estaciones de trabajo, servidores y dispositivos móviles. Con capacidades integrales de control de postura y seguridad: navegación, periféricos, aplicaciones, vulnerabilidades. Incluyendo un EDR para análisis, investigaciones y respuestas más avanzadas.

Secure Mail Gateway:

Protección robusta contra fraudes, phishing y malware en correo electrónico, tanto en Microsoft Office365 como en servidores de correo locales.

Hybrid Cloud Security:

Seguridad optimizada para entornos híbridos, virtualizados y nube.

Incident and Response:

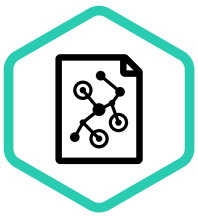
Servicios especializados para la gestión y contención de incidentes, con análisis forense y planes de remediación.

Managed Detection and Response (MDR):

Monitoreo continuo y proactivo 7x24, con expertos que detectan y responden ante amenazas en tiempo real.

Servicios Profesionales:

Consultoría, auditoría y optimización de las tecnologías de Kaspersky para maximizar la eficacia de sus soluciones de ciberseguridad.



Digital Footprint and Brand Protection:

Visibilidad y monitoreo de la huella digital de su organización, incluyendo el análisis continuo y permanente de sus activos expuestos, para anticipar ataques sobre su organización.

Con esta evaluación inicial, usted ya cuenta con un diagnóstico claro de su situación actual.

Nuestro equipo se comunicará a la brevedad para presentarle una propuesta técnica con el detalle y los alcances de cada solución, con el objetivo de avanzar juntos en un plan concreto para madurar la postura de ciberseguridad de su compañía.

Agradecemos nuevamente su confianza,

Atentamente,

Equipo Kaspersky

kaspersky