Siete acciones clave para gestionar los riesgos de ciberseguridad

Los riesgos de **ciberseguridad** son una amenaza creciente para la reputación de las empresas. Las incidencias se han disparado un 2.000% en los últimos meses a causa de la pandemia. Sin embargo, **no llegan al 20% las empresas que han desarrollado protocolos específicos para gestionar la comunicación de crisis por ciberriesgos.**

El *Informe de Riesgos Globales 2020* del Foro Económico Mundial, sitúa los ciberataques a infraestructuras y los ciberataques por robo o fraude de datos o dinero, entre los diez riesgos con mayor expectativa de incremento.

La gestión de los ciberriesgos de reputación recorre distintas fases antes, durante y después de su materialización, en las que se enfrenta diferentes desafíos. Ante ello, **Alberto Alponte, Director de Tecnología de Región Andina de LLYC,** presenta 7 acciones clave para hacer frente a estos desafíos y prevenir ciberataques:

► Sunarp autoriza emisión vía internet de copias informativas de títulos archivados

► Nuevas precisiones sobre el trabajo remoto

► Mesas de Diálogo 2021: Urge ejecutar mejor presupuesto de educación y promover digitalización

1. Anticipar las amenazas, vulnerabilidades y **riesgos de ciberseguridad,** con sus medidas de probabilidad e impacto en la reputación, disponiendo de herramientas específicas de vigilancia y mapeo de ciberriesgos.

2. Contar con sistemas de evaluación de las expectativas de los grupos de interés que permitan una mejor toma de decisiones.

3. Diseñar procesos y guías para la gestión de los distintos escenarios de crisis cibernéticas mediante el entrenamiento en los protocolos, simulacros y técnicas de comunicación específicas.

4. Desarrollar campañas dentro de la empresa para incentivar una cultura de evasión del **ciberriesgo** y educación en temas de protección.

5. Desplegar redes de influencia en las comunidades afines a la empresa y monitorear las opiniones públicas en tiempo real a través de medios de comunicación, redes sociales y encuestas directas, para identificar posibles issues.

6. Posicionar contenidos omnicanal relevantes para la reputación de la compañía en los grupos de interés involucrados.

7. Analizar las causas que originaron la **cibercrisis**, para diagnosticar las medidas correctoras, y planificar las acciones y recursos necesarios para evitar o minimizar el riesgo en el futuro.

Profesionales de la comunicación

Tener estos elementos resulta fundamental en un panorama en que los ciberriesgos de reputación, además, constituyen una preocupación creciente para los profesionales de la comunicación.

Según el *European Communication Monitor 2020* en torno al 45% de profesionales del mundo de la comunicación reconoció el año pasado haber gestionado una crisis por ciberataques en su empresa, apenas un 25,3% indicó haber trabajado en educar a los empleados en la prevención de ciberriesgos y no llegan un 20% los que han desarrollado protocolos específicos para gestionar estos incidentes.

“Es evidente que los riesgos cibernéticos o ciberriesgos representan una amenaza para la continuidad de la actividad o negocio, una potencial pérdida de activos económicos y financieros; pero también lo es que suponen un serio desafío para el capital social y relacional de cualquier entidad», expresó Alponte.

«Si una empresa sufre un ciberataque o incidente y se evidencia que la causa ha sido la falta de medidas de seguridad, tendría un daño reputacional. No se puede esperar a que estas cosas sucedan para actuar, se debe tener un plan de acción y protocolos y realizar análisis de seguridad mensualmente”, finalizó.