

La Comunicación de Crisis como garante reputacional

Eduardo Fuentes // CEO de Grayling España.

Los ciberdelitos salen muy caros a las empresas. Según un reciente informe de Kaspersky, una de las compañías con más experiencia en el sector de la lucha frente al *malware* y el cibercrimen, el coste de una brecha de datos en una pyme europea supera los 73.300 euros mientras que el de una gran empresa se estima en más de 691.000. Un impacto económico que puede verse multiplicado a efectos de consecuencias financieras y de reputación de la empresa u organismo de que se trate si no se informa adecuadamente tanto a públicos internos como externos sobre una brecha de seguridad de datos en el momento oportuno y a través de las vías oportunas.

Y la situación se agrava aún más en un mundo en el que las redes sociales permiten compartir puntos de vista y opiniones a nivel mundial en cuestión de segundos, con lo que la reputación de una organización puede cambiar muy rápidamente gracias a un entorno en el que el contraste de fuentes no existe y con filtros de contenido menos estrictos –por no decir inexistentes– que los de los medios de comunicación tradicionales.

Para que la comunicación sea efectiva en tiempo y forma es clave contar con un protocolo de Comunicación de Crisis perfectamente estructurado que permita actuar ágilmente, y con unos portavoces solventes y bien formados a la hora de saber cómo comunicar durante y tras la crisis. Sufrir el menor menoscabo posible y, sobre todo, poder restaurar la imagen de la compañía tras haber sido dañada, dependen absolutamente de estos dos factores.

El protocolo de Comunicación de Crisis es una herramienta fundamental de la que, desde nuestra experiencia como consultora, carecen –inexplicablemente– muchas compañías, especialmente del entorno de la pequeña y mediana empresa, aunque también se da la situación en un mayor número de grandes firmas del que sería de desear.

Hablamos de un manual exhaustivo, una suerte de guía anticrisis, en el que han de identificarse los tipos de crisis a los que una empresa u organización puede estar expuesta (de procesos de producción, de producto, laboral, social, por regulaciones gubernamentales, financiera, por suplantación de identidad, por desastres naturales, por reclamaciones legales, etc.),



Foto: iStock.com/Pinkyjalis

así como sus características, morfología y nivel de gravedad. Ha de recoger también cómo ha de reaccionarse en cada caso, las medidas a adoptar, su prioridad y operativa, y quién (con nombre, apellidos y cargo) ha de encargarse de qué, tanto a nivel de comunicación interna (empleados) como externa (autoridades, medios, redes sociales y otros *stakeholders*).

Se trata de un manual de extrema utilidad ya que, cuando estalla la crisis, la empresa se convierte de inmediato en un objetivo mediático y todas sus actuaciones sufren un efecto de amplificación. Tanto la compañía como sus máximos responsables –y capacidad de liderazgo– entran en el escrutinio general, tanto de sus propias plantillas y equipos (deben ser tomados como un público preferencial en toda situación de crisis), como de los públicos externos. El daño reputacional puede ser muy grave si no existe una clara asunción por parte de las responsabilidades derivadas de la misma y una gestión comunicativa transparente tanto de la crisis como de la eficacia de las medidas que se pongan en marcha para solventarla.

Habrà que coordinar a la vez muchas áreas y actividades. Entre ellas, comunicar los hechos a los responsables oficiales competentes, localizar a las personas a contactar, evaluar la situación, preparar declaraciones, informar a los empleados, informar a las autoridades que corresponda, responder a los medios de comunicación, monitorizar prensa y redes sociales, recabar informes (internos y externos) y considerar vías de comunicación específicas con proveedores y clientes.

Hablamos de un marco en el que las dos primeras horas que siguen al estallido de la crisis son fundamentales para controlar la situación. Hay que intentar, por todos los medios, que el problema no se magnifique, ni vía prensa, ni vía redes sociales, y contar con que los públicos internos (en muchos casos fuente de controversia si ejercen una portavocía para la que no están preparados o para la que no tienen autorización) estén informados y sean conscientes de su papel y responsabilidad.

Si hay algo que tras más de 25 años de trayectoria profesional en el mundo de la Comunicación he aprendido es que el silencio no es rentable ni eficaz. En situaciones de crisis, menos. Si una empresa elige dar la llamada por respuesta, es muy probable que la versión de “alguien que conoció los hechos” ocupe el lugar que debería ocupar la versión de la empresa. Y ese “alguien” puede ser cualquiera, incluso un competidor con intenciones poco solidarias.

Pero contrarrestar ese silencio no debe entenderse como decir lo primero que se nos ocurra para salir del paso. En este punto, además del manual a que antes hacíamos referencia, es fundamental contar con unos

portavoces solventes, bien formados en materia de Comunicación de Crisis, y preferiblemente del primer cuadro directivo de la compañía, que darán la cara ante los diferentes públicos.

El mantra: dar información tranquilizadora, de calidad, haciendo hincapié en los matices de precisión (que no se limite a una referencia a los hechos, sino que los explique) y dinamismo, lo que requiere a su vez la creación de diversos “puntos informativos” desde donde se suministra información y se atiende con rapidez las solicitudes de medios, poderes públicos, afectados, o, como comentábamos, los propios empleados de la compañía. Nunca, nunca, nunca, mentir o proporcionar información que no esté contrastada al cien por cien.

La transparencia y la verdad (hasta donde se pueda contar) son clave en la resolución de una Comunicación de Crisis en la que, insisto, la empresa debe tomar la iniciativa y ofrecer de manera ágil, puntual y veraz su versión de los hechos como forma de evitar que la prensa o/y otros *stakeholders* magnifiquen la situación. Hay que proyectar una imagen de responsabilidad que, en definitiva, será una de las mejores vías para proteger su reputación. Porque todos somos conscientes de que una crisis puede darse; y las ligadas a ciberdelitos gozan además de un mayor umbral de comprensión por parte del público y del mercado. Pero una mala gestión, resolución o comunicación de esa crisis no es tan bien entendida ni perdonada.

Es complicado dar métricas y cifras que permitan ver cuál es el daño real de una crisis. Pero sí hay indicadores de lo que puede generar una mala comunicación en este área. Si volvemos a los datos analizados por Kaspersky, las empresas que asumen la responsabilidad desde el primer momento suelen conseguir mitigar los daños. Los costes para las pymes que revelan una infracción se estiman en más de 76.500 euros, mientras que en los casos en los que la incidencia llega a los medios a través de una filtración estos daños superan los 127.000 euros. Ocurre lo mismo en las grandes empresas: las que informaron de manera proactiva sobre brechas de seguridad sufrieron un menor impacto financiero (28%) respecto a las que sufrieron una filtración posterior –más de 933.758 euros frente a cerca de 1.304.000 euros–.

En cualquier caso, los costes reputacionales no pueden medirse. Como ya afirmó Warren Buffet, *“Lleva 20 años construirse una reputación y 5 minutos destrozarla. Si piensas en ello, harás las cosas de forma diferente.”* Hacer las cosas de forma diferente pasa, sin lugar a dudas, por estar preparados para afrontar una correcta Comunicación de Crisis. ●