Diálogo *online* organizado por ESTUDIO DE COMUNICACIÓN Y ECIJA: 'Cómo gestionar el riesgo ante una crisis de ciberseguridad y de robo de información'

"LAS EMPRESAS DEBEN DE PROTEGERSE LEGALMENTE Y PROTEGER SU REPUTACION ANTE LOS CIBERATAQUES"

- **Pablo Jiménez de Parga, vicepresidente de ECIJA:** *"*En el segundo trimestre de 2020 casi uno de cada diez usuarios estuvo expuesto a un ciberataque. Hoy, el último ejemplo que tenemos es el del SEPE que afectará al pago regular de las prestaciones de más de 150.000 ciudadanos".
- **Alberto Mariñas, socio de Estudio de Comunicación:** "Las compañías deben de contar con Manuales de Gestión de Crisis que incluya la forma de combatir los ciberataques para preservar su reputación y su imagen pública*".*
- **Julio Collado, *Chief Infomation Security Officer* del Grupo Prisa:** *"*La ciberseguridad no es solo una estructura tecnológica, es una área decisiva en una compañía que incide directamente en el negocio, tan importante como cualquier otra área*".*
- **María José Gallego, Data Protection Officer de Orange en España:** "Las brechas de seguridad, de información y otro tipo de vulnerabilidad de datos, deben contar con protocolos claros de actuación para poder tener una reacción lo suficientemente ágil por parte de las compañías, siempre en estrecha colaboración entre las áreas de Ciberseguridad y DPO."
- **Alonso Hurtado, socio IT&Compliance de ECIJA:** "Cualquier brecha de seguridad tiene que tener una respuesta coordinada jurídica, tecnológica y de comunicación".
- **Jesús Yáñez, socio de IT&Compliance de ECIJA:** "Va a haber ayudas económicas destinadas a la cibeseguridad provenientes de los Fondos Europeos, además del Plan nacional español dentro del Programa Activa Ciberseguridad y las subvenciones a nivel autonómico".

Madrid, 24 de marzo de 2021. – **Pablo Jiménez de Parga,** vicepresidente de **ECIJA, y Alberto Mariñas,** socio de **Estudio de Comunicación,** han presentado el encuentro *online* "Cómo gestionar el riesgo ante una crisis de ciberseguridad y de robo de información", que ha contado con expertos como **Julio Collado**, *Chief Information Security Officer* del **Grupo Prisa**, **María José Gallego**, *Data Protection Officer* de **Orange España** y **Alonso Hurtado** y **Jesús Yáñez,** socios de IT&Compliance de **ECIJA**.

Pablo Jiménez de Parga destacó que "la ciberseguridad se ha vuelto una asignatura esencial para todo tipo de empresas e instituciones. El auge de todo tipo de dispositivos tecnológicos, cada vez más sofisticados, la globalización y también el anonimato que permite operar en Internet está provocando que el número de ciberataques se encuentren en constante aumento. La pandemia, con miles de empleados en teletrabajo conectados desde fuera del entorno de seguridad corporativo, ha propiciado los ataques de los *hackers* exponencialmente".

Jimenez de Parga afirmó que estos ataques ponen en juego datos sensibles de ciudadanos, clientes y de las propias organizaciones y, al mismo tiempo, inciden negativamente en la reputación de los atacados y pueden llegar a ser fuente de reclamación de terceros: *"*En el segundo trimestre de 2020 casi uno de cada diez usuarios estuvo expuesto a un ciberataque, como es el caso del SEPE que afectará al pago regular de las prestaciones de más de 150.000 ciudadanos. Por ello, es necesario contar con planes de protección desde el punto de vista legal, de imagen y reputación para proteger los intereses de empresas e instituciones".

Por su parte**, Alberto Mariñas, Socio de Estudio de Comunicación**, explicó que "la reputación es algo que sufre mucho con la ciberseguridad". Desde el punto de vista de la comunicación, Mariñas defiende que es esencial la planificación por lo que recomienda a las compañías contar con un Manual de gestión de crisis que incluya la forma de combatir los ciberataques. En su opinión "el Manual de Crisis es una herramienta que te permite ganar tiempo, ser más eficaces y tener contempladas todas las posibles salidas". También resaltó la importancia de "incluir nuevos elementos en la cultura de las empresas con técnicas de dinamización y motivación como un buen proceso de comunicación interna".

Julio Collado, *Chief Information Security Officer* del Grupo Prisa, explicó que la ciberseguridad ha existido siempre "pero no con el protagonismo tan relevante de hoy, en que ya no es solo una estructura puramente tecnológica, sino que es tan importante decisiva en una compañía e incide directamente en el negocio". También puso de relevancia la importancia de la concienciación en las prácticas de buen gobierno de cualquier compañía, y de la concienciación de los directivos. Así mismo ensalzó "la figura del DPO (Delegado de Protección de Datos o Privacidad) que considera imprescindible en la empresa actual".

María José Gallego, *Data Protection Officer* de Orange en España, comentó en su intervención que la implementación de medidas técnicas básicas en las organizaciones, como puede ser la suscripción a alarmas deberían ser de obligado cumplimiento porque no suponen una gran inversión pero tienen una importante efectividad. Gallego puso especial hincapié en la necesidad de sensibilizar a los empleados ante posibles incidentes de seguridad, y en la importancia de la formación y concienciación en las compañías. Las brechas de seguridad, de información y otro tipo de vulnerabilidad de datos, deben contar con protocolos claros de actuación para poder tener una reacción lo suficientemente ágil por parte de las compañías, siempre en estrecha colaboración entre las áreas de Ciberseguridad y DPO."

A juicio de **Alonso Hurtado, socio de IT&Compliance de ECIJA**, "cualquier brecha de seguridad tiene que tener una acción coordinada de comunicación, jurídico y tecnológico. Desde el punto de vista reputacional se pude ver afectada la imagen de una compañía en los medios de comunicación y, además, podemos ser víctimas de una sanción económica". En el caso concreto del SEPE, **Hurtado** aclaró que la clave estará en la capacidad que tenga de demostrar que ha sido diligente en las medidas que ha llevado a cabo antes y después del ciberataque y en acreditar que ha cumplido con la ley. "Desde el punto de vista procesal esto será clave", ha concluido.

Jesús Yáñez, socio de IT&Compliance del mismo despacho, explicó que la normativa en temas de ciberseguridad ha evolucionado muchísimo y que "ahora se regulan en España y en Europa sectores que antes no lo estaban y no solo las multinacionales cuentan con mecanismos de protección sino también las pymes". Según Yáñez es esencial contar con una infraestructura tecnológica y con medidas de seguridad del sistema nacional. Yañez aseguró que "sí va a haber ayudas económicas destinadas a la ciberseguridad provenientes de los Fondos Europeos". Actualmente -explicó- ya existe un Plan nacional de ayudas dirigidas a impulsar la aplicación de la ciberseguridad en las pequeñas y medianas empresas españolas en el marco del Programa Activa Ciberseguridad, y además existen subvenciones a nivel autonómico.

Para más información:
vmagro@estudiodecomunicacion.com
csotomayor@estudiodecomunicacion.com
915765250