



Hiscox CyberClear 360° Para Administradores de Fincas Colegiados

Hiscox CyberClear 360° ha sido diseñado específicamente para dar soporte y proteger ante los riesgos cibernéticos de empresas de todo tipo de tamaño.

Un ataque puede afectar a miles de equipos por todo el mundo, independientemente del tamaño. Pymes y gran empresa pueden ver su negocio bloqueado por la imposibilidad de acceder a sus equipos informáticos o perder datos de gran valor.

Las normas de protección de datos son cada vez más estrictas y las sanciones más severas, lo que pone en peligro la viabilidad de muchos negocios.

La póliza de Hiscox CyberClear 360° es mucho más que un seguro. Le da acceso a una serie de servicios y herramientas sin coste adicional para ayudarle a gestionar mejor su riesgo.

Servicios de ciberseguridad Hiscox

Una suite de herramientas para mejorar la ciber preparación de su empresa que incluye: servicios para configurar capas adicionales de seguridad, informes de su presencia en Internet, sistemas de almacenamiento para copias de seguridad, revisión, puesta a punto y localizador de dispositivos, borrado digital, soporte para Office 365 y GSuite.

Servicio de Respuesta a Incidentes

Servicios de contención tecnológica para mitigar el posible daño con las siguientes acciones

- Asesoramiento sobre cómo detener o contener un incidente
- Establecer, en la medida de lo posible, la causa y el alcance de un incidente
- Confirmar la ocurrencia de una vulneración de datos, e identificar, en la medida de lo posible, a los afectados
- Emitir las recomendaciones oportunas para evitar la repetición del incidente, siempre y cuando la causa haya podido ser detectada

Servicio de asesoramiento jurídico, de comunicación y relaciones públicas.

- El servicio de asesoramiento jurídico externo para asesorar sobre las actuaciones que deben ser tomadas para gestionar la respuesta al incidente, cuando sea necesario.
- Gastos de relaciones públicas, entendidos como los servicios:
 - de un consultor especializado en ayudar al asegurado a restablecer su reputación y gestionar su comunicación externa derivado de un incidente, incluyendo el desarrollo y comunicación de una estrategia para dicho fin, cuando sea necesario
 - para emitir comunicados vía correo electrónico o en su sitio web y redes sociales
 - cualquier otra medida razonable y proporcionada para restablecer su reputación, con nuestro consentimiento previo por escrito.

Gastos de notificación y monitorización

- gastos para notificar a cualquier entidad reguladora, u otras autoridades competentes la vulneración de datos, siempre que el asegurado esté legalmente obligado a hacerlo, con nuestro previo consentimiento
- gastos de uso de un centro de atención telefónica externo para responder a consultas de los afectados, previamente notificados, a consecuencia de una vulneración de datos, con nuestro previo consentimiento
- gastos de monitorización de la identidad: la contratación de un servicio de monitorización de la información comprometida de los afectados, en sitios públicos de Internet, con el fin de evitar un uso inadecuado, durante un periodo máximo de

un año desde la fecha de activación. El servicio deberá activarse únicamente tras la notificación, previo acuerdo con la aseguradora, a los afectados a consecuencia de una vulneración de datos

- gastos para notificar a los afectados la vulneración de datos, con nuestro previo consentimiento
- gastos por monitorización de crédito: reembolso de los gastos razonables y necesarios incurridos por la entidad, con nuestro previo consentimiento, para la contratación de un servicio de monitorización de crédito o similar para los afectados, previamente notificados, a consecuencia de una vulneración de datos

Extensión de cobertura para sistemas alojados en la nube de un proveedor externo tecnológico

Se hace constar que quedan cubiertos en los mismos términos, el servicio de respuesta a incidentes en caso de un incidente que afecte a un sistema:

- usado por la entidad para el desarrollo de su actividad y para su propio beneficio
- que sea facilitado por un proveedor externo tecnológico
- que esté alojado en la nube de un proveedor externo tecnológico;

Pérdidas del asegurado

Si durante el periodo de seguro el asegurado descubre un incidente, real o presunto, la aseguradora abonará los gastos incurridos, con el consentimiento previo por escrito de la aseguradora para:

Gastos de recuperación de datos o sistemas

- recuperar el acceso a los programas, sistema informático, o datos electrónicos de la entidad;
- reconfigurar, instalar a partir de copias de seguridad, copias originales u otras fuentes o, en caso de ser necesario, sustituir un programa de terceros (legalmente adquirido) en el sistema informático
- recrear los datos electrónicos de la entidad
- gastos de mitigación.

Extorsión cibernética

La aseguradora reembolsará:

- el importe económico del rescate pagado por el asegurado o, si el tercero ha exigido el pago del rescate en la forma de bienes o servicios, el valor de mercado de dichos bienes o servicios en el momento de la entrega del rescate
- los honorarios y otros gastos incurridos por un consultor especializado para ayudar al asegurado en la gestión y negociación del rescate
- el importe de un rescate robado por un tercero, siempre que dicho robo ocurra en el lugar acordado para el pago del rescate, o de camino al mismo
- gastos de mitigación.

Protección de equipos

Hasta el sublímite indicado en las condiciones particulares, reembolsaremos a la entidad, el coste de reparación o sustitución de un equipo informático (hardware o móvil) que forme parte del sistema informático y sea de su propiedad, usado para el desarrollo de su negocio, incluyendo pero sin limitarse a ordenadores, servidores, teléfonos, smartphones, tablets, televisores, impresoras, escáneres, cámaras, sensores, altavoces inteligentes y otros dispositivos conectados a Internet, siempre y cuando:

- los equipos informáticos contengan datos personales, información confidencial o información corporativa de la entidad
- los equipos informáticos hayan sido afectados por un incidente y ya no puedan ser usados para las funciones para las cuales se destinaban;

Responsabilidad tecnológica

Si, durante el periodo de seguro el asegurado a consecuencia de un incidente:

Recibe una reclamación alegando:

- incumplimiento, violación o infracción involuntaria de cualquier normativa de **protección de datos personales** o derecho a la privacidad, siempre y cuando, la reclamación no esté basada directa o indirectamente en la recogida y/o el

tratamiento de datos personales por la entidad, o por cualquiera que actúe en su nombre, sin haber obtenido previamente el consentimiento suficiente con respecto al marco legal o regulatorio. Se hace constar que se da cobertura bajo esta sección a las reclamaciones presentadas por los empleados, en el caso de que sus datos personales se hayan visto vulnerados. No se cubren reclamaciones presentadas por cualquier socio, administrador o directivo.

- incumplimiento de cualquier deber de confidencialidad de datos personales o información confidencial
- incumplimiento de cualquier deber contractual para mantener la seguridad o confidencialidad de datos personales, información confidencial o información corporativa, incluyendo un incumplimiento de la política de privacidad de la entidad.
- Es objeto de una **inspección de datos o de cualquier otro procedimiento normativo en materia de protección de datos**.
- Es objeto de un procedimiento por incumplir con el estándar de seguridad de los datos de la Industria de las tarjetas de pago (en inglés: payment card industry data security standard).
- Recibe una reclamación derivada directamente de la modificación por parte de un tercero o de un empleado (excluyendo socios, administradores o directivos) y como consecuencia de un ciberataque del contenido del correo electrónico, redes sociales, intranet, extranet o sitio web de la entidad.
- Recibe una reclamación basada en la transmisión de un virus, en un acceso o uso no autorizado del Sistema informático de un tercero o en un ataque de denegación de servicio a un tercero, realizado a través o utilizando el sistema informático de la entidad.

Suplantación de Identidad en cuenta bancaria

La aseguradora abonará la suplantación de identidad en cuenta bancaria descubierta por primera vez durante el periodo de seguro, hasta el límite de indemnización indicado en las Condiciones Particulares en el apartado de “Suplantación de identidad”. Dicho límite formará parte del límite de indemnización agregado de la cobertura 2.4. Fraude tecnológico y nunca en adición al mismo.

Se entiende por Suplantación de identidad en cuenta bancaria la pérdida financiera directa de la entidad causada por un ataque de ingeniería social y que se produzca por una transferencia de fondos, o la instrucción para dicha transferencia, realizada desde una cuenta bancaria por una persona asegurada de buena fe, 1) alterando los datos bancarios de un cliente, proveedor o prestador de servicios o 2) en el caso de suplantación de una persona asegurada, siguiendo las instrucciones fraudulentas de la persona que realiza el ataque de ingeniería social.

Suplantación de identidad en cuentas bancarias de comunidades de propietarios

Ampliación de la cobertura de suplantación de identidad a la cobertura de suplantación de identidad en cuentas bancarias de comunidades de propietarios? Sí No

En caso afirmativo, conteste a las siguientes cuestiones:

- En caso de solicitud de cambio de los números de cuenta, ¿Se verifica con la persona contacto que dicha solicitud de cambio es legítima mediante un medio distinto al que recibió la solicitud de cambio (por ejemplo se reciba por email y se verifica telefónicamente)? Sí No
- ¿Verifica semanalmente en sus cuentas bancarias que los movimientos de la misma (conciliación bancaria) hayan sido efectivamente realizados por usted? Sí No

Resumen del proyecto y coberturas

GARANTÍAS	LÍMITE	FRANQUICIAS
Servicio de Respuesta a Incidentes	300.000 €	1.500 € por incidente
Gastos de Mitigación	45.000 €	0 €
Ciber Extorsión	300.000 €	0 €
Gastos de Recuperación de Datos y Sistemas	300.000 €	0 €
Protección de Equipos	45.000 €	1.000 € por incidente
Responsabilidad Tecnológica	300.000 €	0 €
Fraude Tecnológico	45.000 €	0 €
Suplantación de identidad incluida las cuentas bancarias de las comunidades.	a) 15.000 € b) 25.000 € c) 50.000 €	1.000 € por pérdida

PRIMA TOTAL ANUAL*	597 €
---------------------------	--------------

Prima calculada para un Administrador de Fincas cuya facturación anual en honorarios está entre 150.000 € y 200.000 € con el límite a) de suplantación de identidad.