¿Está preparado para el ransomware?

El coste medio de subsanar los efectos del ataque de ransomware más reciente es de **602 287 Euros** para las organizaciones que no pagan el rescate y asciende a los **1 194 180 Euros** para las que sí lo pagan[1]

Lea este libro electrónico para aprender a minimizar la vulnerabilidad de su organización al ransomware.

StorageCraft.

¿Qué es el **ransomware**?

El ransomware es un tipo de software malicioso que le impide acceder a sus datos hasta el pago de un rescate.

Los ataques de ransomware han aumentado un 40 % en 2020, lo que se ha traducido en 199,7 millones de ataques.[2]

Este incremento se ha visto avivado por el auge del "ransomware como servicio". Este tipo de ransomware se ha diseñado para su uso por personas con un conocimiento técnico mínimo o nulo. El ransomware se ha convertido en un negocio en todo el mundo impulsado por las mafias internacionales.

Estos agentes solo tienen que descargar el virus de manera gratuita o tras el pago de un precio simbólico, fijar un rescate y una fecha límite para el pago e intentar engañar a alguien para infectar su ordenador. Si la víctima realiza el pago, el autor original recibe una parte (aproximadamente entre el 5 y el 20 %) y el resto va directo al "aprendiz de hacker" que haya lanzado el ataque.

StorageCraft.

El 75 % de las organizaciones infectadas con ransomware ejecutaban protección de extremo actualizada[3]

Teniendo en cuenta el nivel de ingresos que genera, se puede afirmar con rotundidad que no se trata de una tendencia pasajera. Para mantener la seguridad y fortaleza de su empresa, ha de estar al tanto de los riesgos y adoptar las medidas pertinentes y necesarias.

Ransomware
Los datos

51 % de las organizaciones se han visto afectadas por el ransomware en el último año[1]

StorageCraft

62 %

El 62 % de las pequeñas y medianas empresas se han visto afectadas por el ransomware[4]

€ 16 500 millones

Costes globales previstos por daños debidos al ransomware **en 2021**[5]

197 días

Las empresas identifican que han sufrido una vulneración de la seguridad de sus datos tras una media de 197 días[6]

62 %

El 62 % ha recibido una solicitud de pago de un rescate[7]

66 %

Solo el 66 % de las empresas que han pagado el rescate han podido recuperar sus datos[7]

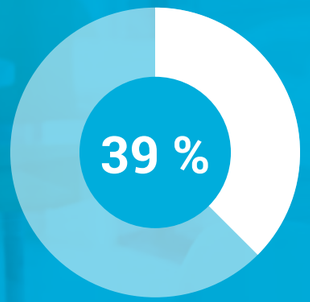
15,7 días

Duración media de un incidente con origen en el ransomware[4]

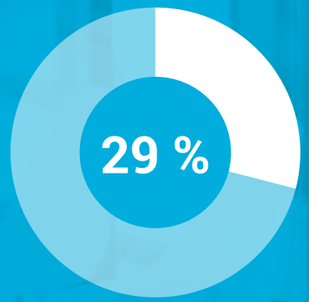
11 segundos

En 2021, se producirá un ataque cada 11 segundos[5]

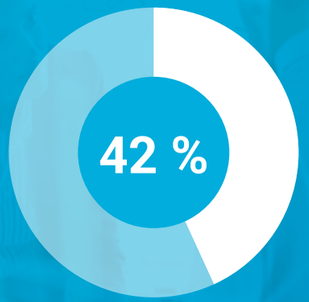
El ransomware se aprovecha del eslabón más débil: **sus empleados**[8]



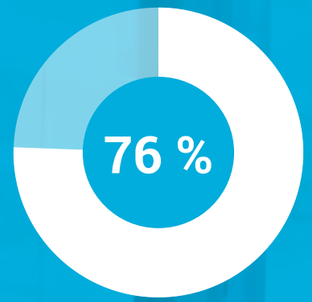
El 39 % de las organizaciones que se han visto afectadas por el ransomware afirma que llegó a través de un correo electrónico



El 29 % de las empresas afirma que el ataque se realizó a través de su personal de menor rango



El 42 % se realizó a través de los responsables de rango intermedio



El 76 % de los adultos de Reino Unido no saben qué es el ransomware

Inculque a **todos** la responsabilidad en la defensa contra el ransomware.

Paso 1

Instruya a sus empleados

Entre las prácticas recomendadas deben figurar las siguientes:

Analice los enlaces que contengan los correos electrónicos y no abra los archivos adjuntos incluidos en los correos electrónicos no solicitados.

Únicamente descargue software (especialmente, el software gratuito) de sitios conocidos y de confianza. En la medida de lo posible, verifique la integridad del software a través de la firma digital antes de ejecutarlo.

Invierta en formar a su personal, con objeto de que conozcan cómo actúa el ransomware (incluido el phishing).

Paso 2

Acciones para el departamento de TI/ proveedor de servicios de TI

Instruya a los usuarios finales para que no abran correos electrónicos ni archivos adjuntos procedentes de remitentes desconocidos ni descarguen software de sitios de torrents, y que limiten sus actividades de navegación solo a aplicaciones y sitios web aprobados.

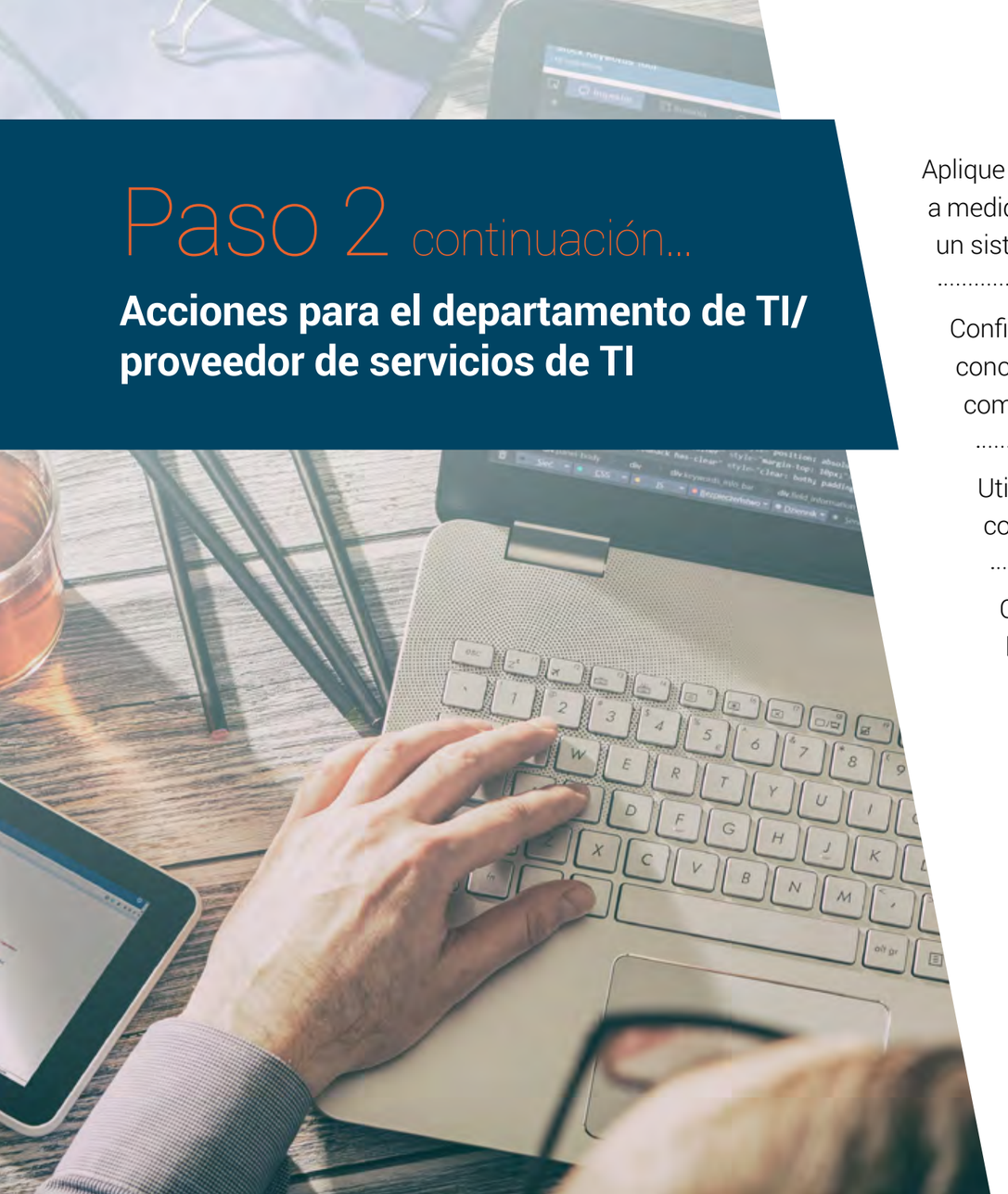
Controle los derechos de administración a los datos esenciales de la empresa. Mantenga los sistemas operativos parcheados y actualizados con regularidad. Implemente firewalls y herramientas de seguridad de correo electrónico de última generación para bloquear los ataques de phishing. Instale y habilite un antivirus basado en firmas o software AV de última generación.

Garantice que los parches de aplicaciones para el sistema operativo, el software y el firmware estén actualizados, lo que incluye Adobe Flash, Java, navegadores web, etc.

Asegúrese de que las soluciones antivirus y antimalware estén configuradas para que se actualicen automáticamente y de que se realicen análisis periódicos.

Desactive los scripts de las macros de los archivos enviados a través del correo electrónico. Plantéese utilizar el software Office Viewer para abrir los archivos de Microsoft Office enviados a través del correo electrónico en lugar de utilizar las aplicaciones del conjunto completo de Office.

Implemente restricciones de software u otras medidas de control para evitar que se ejecuten programas en ubicaciones frecuentes que ocupa el ransomware, como las carpetas temporales de los navegadores de Internet generales o programas de compresión/ descompresión, incluidos los de la carpeta AppData/LocalAppData.



Paso 2 continuación...

Acciones para el departamento de TI/ proveedor de servicios de TI

Aplique parches en todos los sistemas operativos de los dispositivos de extremo, el software y el firmware a medida que se detecten las vulnerabilidades. Esta medida de precaución se puede facilitar a través de un sistema de administración centralizada de parches.

Configure controles de acceso con los privilegios mínimos. Si un usuario solo tiene que leer archivos concretos, no tiene por qué contar con acceso de escritura a dichos archivos, directorios o recursos compartidos.

Utilice entornos virtualizados para ejecutar los entornos de los sistemas operativos o programas concretos.

Categorice los datos en función del valor para la organización e implemente una separación física/ lógica de las redes y los datos en las distintas unidades organizativas. Por ejemplo, los datos confidenciales de investigaciones o de la empresa no deben encontrarse en el mismo servidor o segmento de red que el entorno de correo electrónico de una organización.

Solicite la interacción del usuario en las aplicaciones de usuario final que se comunican con sitios web no categorizados por el firewall o proxy de red. Algunos ejemplos son solicitar a los usuarios que escriban información o introduzcan una contraseña cuando el sistema se comunica con un sitio web no categorizado.

Implemente listas blancas en las aplicaciones. Permita únicamente que los sistemas ejecuten programas conocidos y permitidos por la política de seguridad.

Paso 3

Implemente un plan de recuperación tras desastres

A pesar de todas las medidas preventivas que adopte, ha de prever la posibilidad de que el ataque surta efecto.

“Nosotros mismos sufrimos un ataque que no se debió a nuestro descuido precisamente. Ante un ataque dirigido, las medidas preventivas pueden quedarse cortas (y así sucede con frecuencia). Cuando esto ocurre, ha de tener implementado un plan de recuperación tras desastres.”

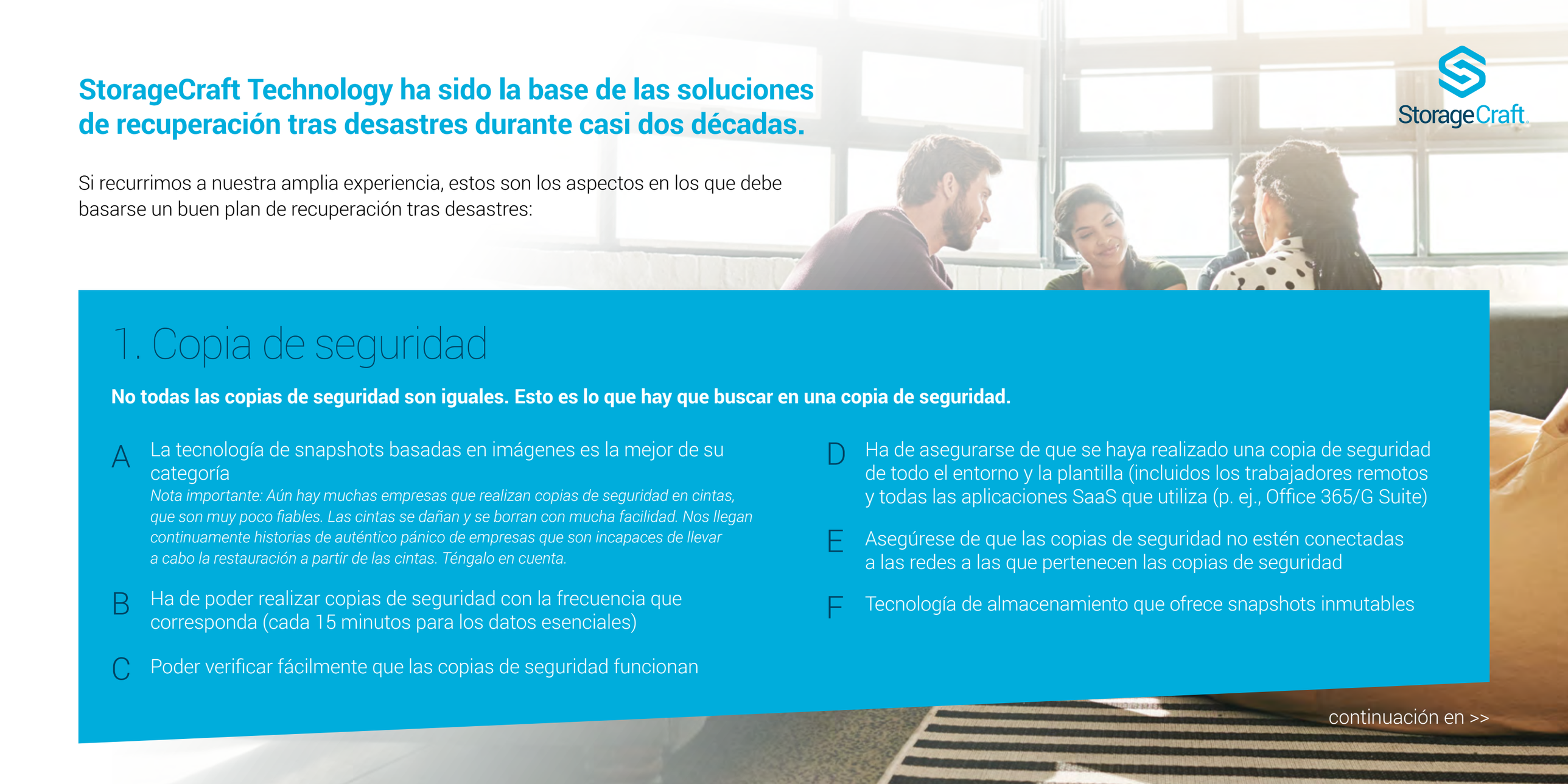
Jonathan Anstee - Scott Aerospace

Scott Aerospace luchó con éxito contra un ataque de ransomware dirigido gracias a StorageCraft Technology como parte de su plan de recuperación tras desastres.

El plan de recuperación tras desastres es su **última línea de defensa**.

StorageCraft Technology ha sido la base de las soluciones de recuperación tras desastres durante casi dos décadas.

Si recurrimos a nuestra amplia experiencia, estos son los aspectos en los que debe basarse un buen plan de recuperación tras desastres:



1. Copia de seguridad

No todas las copias de seguridad son iguales. Esto es lo que hay que buscar en una copia de seguridad.

A La tecnología de snapshots basadas en imágenes es la mejor de su categoría
Nota importante: Aún hay muchas empresas que realizan copias de seguridad en cintas, que son muy poco fiables. Las cintas se dañan y se borran con mucha facilidad. Nos llegan continuamente historias de auténtico pánico de empresas que son incapaces de llevar a cabo la restauración a partir de las cintas. Téngalo en cuenta.

B Ha de poder realizar copias de seguridad con la frecuencia que corresponda (cada 15 minutos para los datos esenciales)

C Poder verificar fácilmente que las copias de seguridad funcionan

D Ha de asegurarse de que se haya realizado una copia de seguridad de todo el entorno y la plantilla (incluidos los trabajadores remotos y todas las aplicaciones SaaS que utiliza (p. ej., Office 365/G Suite)

E Asegúrese de que las copias de seguridad no estén conectadas a las redes a las que pertenecen las copias de seguridad

F Tecnología de almacenamiento que ofrece snapshots inmutables

continuación en >>

Los aspectos en los que debe basarse un buen plan de recuperación tras desastres (continuación)

2. Replicación externa

Es fundamental que replique las copias de seguridad de manera externa para garantizar la continuidad de negocio en caso de que se produzca un problema en las instalaciones.

Es posible que las copias de seguridad locales no sean suficientes en caso de que un ransomware más destructivo ataque las carpetas compartidas en los servidores NAS accediendo a los servicios de archivo de los ordenadores. La mejor manera de evitarlo es tener almacenadas versiones sin infectar de las copias de seguridad almacenadas en una ubicación externa.

Una buena solución de recuperación tras desastres ha de replicar los datos en la ubicación que elija (quizás en una segunda ubicación en la empresa o en una nube pública o privada) y hacerlo en función de una programación que se adapte a sus necesidades.

3. Pruebas

DEBE poder poner a prueba su plan de recuperación tras desastres. No permita que un desastre sea su primera prueba.

Un buen plan de recuperación tras desastres ha de ponerse a prueba con facilidad (y con frecuencia).

Es la única manera en que puede validar que se cumplan los objetivos de tiempo de recuperación.

4. Recuperación

Puede parecer obvio, pero, por desgracia, es en este punto donde fallan las denominadas "soluciones de recuperación tras desastres". La recuperación tras desastres debe poder recuperar sus datos en todo momento y a tiempo.

Cuando tenga lugar un desastre como el ransomware, querrá tener plena seguridad en que podrá recuperar sus datos y seguir trabajando.

Conclusión

No existe ninguna receta milagrosa a la hora de lidiar con el ransomware. El mejor enfoque se divide en varios niveles, es decir, que incorpore la instrucción del personal, mantenga actualizado el software antivirus, aplique con frecuencia parches al software y, lo más importante, disponga de un plan de recuperación tras desastres sólido y probado.

Las potentes soluciones de continuidad de negocio, administración y protección de datos de StorageCraft permiten una recuperación de datos completa, instantánea y fiable en caso de un ataque de ransomware exitoso y eliminan el tiempo de inactividad.

Para obtener más información, visite
www.storagecraft.com/es/ransomware

La continuidad de negocio comienza aquí.

Contacto

Póngase en contacto con el departamento de ventas por correo electrónico

América	sales@storagecraft.com
Asia Pacífico	**Australia:** sales@storagecraft.com.au **Nueva Zelanda:** sales@storagecraft.co.nz **Este y Sureste de Asia:** sales-asia@storagecraft.com
Europa	sales@storagecraft.eu

En España, IREO es mayorista de las soluciones de StorageCraft

Le pondremos en contacto con un distribuidor autorizado para acceder a la información que necesite sobre las soluciones de StorageCraft.
info@ireo.com

Fuentes

[1] Sophos - State of Ransomware 2020 Whitepaper

[2] Security Magazine (octubre de 2020)

[3] 2020 Cyber Security Statistics, PurpleSec

[4] Beazley Breach Brief 2020

[5] Cyber Security Ventures (artículo sobre los cinco principales datos, figuras, predicciones y estadísticas sobre ciberseguridad para 2019-2021)

[6] Artículo del blog de Varonis sobre los tiempos de respuesta frente a las vulneraciones de seguridad de los datos

[7] Corporate Compliance Insights - Ransomware attacks spike; organisations agree to pay

[8] IT Governance UK - “Ransomware attacks strike hard...”