CCN
centro criptológico nacional

10 CLAVES PARA LA PREVENCIÓN PROACTIVA

Hoy en día no vale esperar a que pase algo, hay que **ser proactivos**, ser más **vigilantes y** tener más **capacidad adaptativa**.

La experiencia y autoconocimiento nos dan los medios para anticiparnos a las amenazas, reducir el riesgo, a la vez que dosificar y focalizar los esfuerzos.

1

Utiliza **autenticación multifactor** en los servicios a los que accedes a distancia y aplicaciones que lo permitan, como VPN, VDI, correo electrónico, redes sociales… Además, considera el uso de tokens resistentes a la suplantación de identidad, como tarjetas inteligentes y claves de seguridad FIDO2 (Fast IDentity Online).

2

Cambia las **contraseñas** que vienen por defecto por credenciales robustas y nunca las reutilices. Utiliza el gestor de contraseñas corporativo para ayudarte a gestionarlas.

3

Mantén el **software actualizado** en todos tus dispositivos, tanto profesionales como personales, para prevenir vulnerabilidades. También es necesario rediseñar los procesos para distribuir parches de criticidad alta lo antes posible.

4

Controla estrictamente **los accesos** del personal y especialmente de terceros. Es recomendable el empleo de restricciones de red utilizando atributos adicionales como la información del dispositivo, el entorno y las rutas de acceso.

5

Revisa tu estrategia de **copias de seguridad**. Realízalas periódicamente, sobre todo de datos críticos, y asegúrate que el acceso a las mismos está controlado. Recomendamos el enfoque 3-2-1 (mantener 3 copias completas + 2 almacenadas localmente en diferentes medios + 1 copia fuera de las instalaciones).

Más información aquí

6

Organiza **sesiones de concienciación** para tus empleados en materia de ciberseguridad, haciendo especial hincapié en ataques de ingeniería social, **y capacitaciones** sobre políticas y procedimientos de seguridad específicos para usuarios administradores.

7

Activa el **filtro antispam** para crear un entorno de seguridad en tu correo electrónico para evitar la llegada de mensajes maliciosos.

8

Protege tus activos **de ataques de denegación de servicio** usando una CDN (Red de distribución de contenidos) con funciones de alta disponibilidad de las plataformas en la nube.

9

Bloquea o limita el acceso a internet de **servidores o dispositivos que no suelen reiniciarse**. Pueden crearse puertas traseras y elementos persistentes a través de ellos, lo que supone una oportunidad perfecta para los ciberdelincuentes.

10

Asegúrate de que dispones de los procedimientos necesarios y canales para **comunicarte rápidamente con tu CSIRT**.

Puedes encontrarlos aquí.

CCN-CERT
centro criptológico nacional