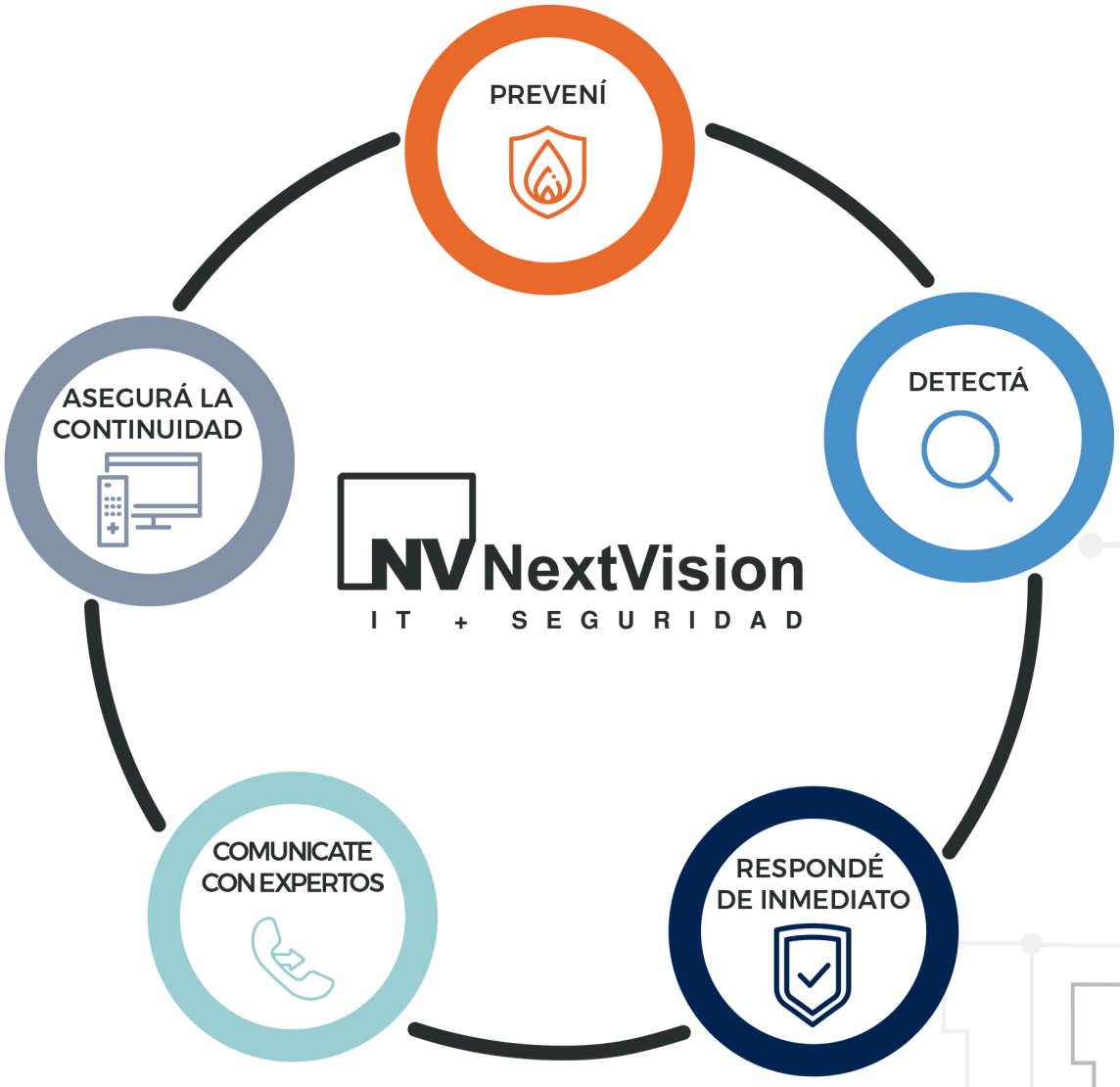
NV NextVision
IT + SEGURIDAD

RANSOMWARE

¿TU ORGANIZACIÓN ESTÁ PREPARADA PARA ENFRENTARSE A ESTA AMENAZA?

Te decimos cómo actuar en cada fase para no sufrir ante un ataque



NextVision
IT + SEGURIDAD

PREVENÍ

- Mantené tu **antimalware** actualizado con tecnología Machine Learning y activá el IPS de tu solución.
- Tené un **Firewall** activo con reglas y políticas de seguridad.
- Instalá **tecnología Antispam** que te permita bloquear correos sospechosos y archivos adjuntos ejecutables.
- Usá un **filtro web** para evitar los sitios comprometidos.
- Adoptá **políticas de grupo (GPO)** para controlar la ejecución de programas.
- Mantené al día la instalación de **parches de seguridad** de los programas que usás para evitar la explotación de vulnerabilidades.
- Aplicá **restricción de cuentas y derechos administrativos**.
- Implementá un sistema de prevención de intrusiones **(IPS)** .

¡Educá! La mejor prevención es concientizar a tus empleados en el uso prudente de Internet.

NextVision
IT + SEGURIDAD

DETECTÁ

- Implementá Tecnología **Sandbox** para explotar posibles vulnerabilidades de programas en un ambiente aislado.
- Usá un sistema de detección de intrusiones **(IDS)** para estar alerta ante actividades sospechosas en tu red.
- Integrá Tecnologías de **Análisis de Comportamiento** para detectar procesos anómalos en tiempo real.
- Usá la **correlación de eventos** para tener un contexto más amplio de las actividades en la red y poder responder mejor ante posibles ataques.

NextVision
IT + SEGURIDAD

SI SE ACTIVÓ UN ATAQUE...

RESPONDÉ DE INMEDIATO

- **Consultá el Plan de Contingencia (si existiera en la organización)**
- **Aislá la amenaza**
  - Remové el Ransomware con las nuevas firmas de tu Antimalware actualizado.
    - ¡Ojo! No vas a poder desencriptar los archivos infectados.
  - Recuperá los archivos secuestrados con tu Backup: te recomendamos tener un soporte físico para tu backup, ya que los respaldos en la nube pueden ser afectados ante un ataque.

NV NextVision
IT + SEGURIDAD

SI SE ACTIVÓ UN ATAQUE...

COMUNICATE CON EXPERTOS EN CIBERSEGURIDAD

- Evaluá el riesgo de propagación junto con ellos.
- Enviáles la nota de rescate recibida y un ejemplo de archivo encriptado (de ser posible)

¡NO PAGUES EL RESCATE!

No existen garantías de que podrás recuperar tus datos y estás alimentando organizaciones cibercriminales.

NextVision
IT + SEGURIDAD

DESPUÉS DEL ATAQUE ...

ASEGURÁ LA CONTINUIDAD DE LA OPERACIÓN

- Garantizá siempre el acceso remoto a los sistemas.
- Contá con **Backup confiable**
  - Hacé verificaciones periódicas.
  - **Duplicá tu Backup** y tu alojamiento de **cintas en sitios externos.**
- Chequeá que el ambiente productivo esté protegido contra amenazas similares.
- **Mantené actualizada la documentación de:**
  - Red
  - Servicios de infraestructura
  - Políticas de autenticación
  - Servicios de seguridad
  - Plan de Contingencia y procedimientos

¡El Ransomware no solo infecta los endpoints!

Todos los dispositivos pueden ser afectados:

- Tablets
- Celulares
- Servidores
- Máquinas virtuales
- Dispositivos con firmwares
- IOT

NextVision
IT + SEGURIDAD

TENÉ EN CUENTA

- El 97% de los ataques se pueden evitar con controles de seguridad estándar (Fuente: Verizon)
- Un 43% de las víctimas de Ransomware son organizaciones (Fuente: Symantec)
- El Email es el primer vector de ataque (Fuente: Kaspersky)
- Solo el 37% de las empresas reconoce tener un plan de respuesta ante un ataque informático (Fuente: Informe PwC 2017)

La mejor manera de empoderar tu organización ante las ciberamenazas es la:

Ciber Resiliencia

Una organización ciber resiliente es capaz de adaptarse y responder ante las amenazas. Administra los riesgos, puede recuperarse de forma ágil y mantener la operación en caso de haber sufrido un ataque.

NextVision

IT + SEGURIDAD

Quiénes somos:

Somos especialistas en Ciberseguridad y Tecnología. Colaboramos para que la información de nuestros clientes en LATAM y España esté siempre protegida y disponible. Trabajamos en la detección, respuesta y remediación de crisis aportando innovación en cada una de nuestras soluciones.