Español

Guía de Seguridad IT para Empresas — Explicada por NetGuard Solutions

En NetGuard Solutions trabajamos todos los días protegiendo redes de empresas de distintos tamaños e industrias. Sabemos que muchos de nuestros clientes no son expertos en tecnología, y está bien: **nuestro objetivo es ayudarles a entender lo esencial para mantener su empresa segura**.

Por eso preparamos esta guía simple y directa con las mejores prácticas de seguridad recomendadas por organizaciones internacionales. Cada punto incluye un enlace para que puedan consultarlo por su cuenta y aprender más si lo desean.

---

1. Verificar primero, confiar después (Zero Trust)

En seguridad, lo más importante es **no dar acceso automático a nada ni a nadie**. Todo debe verificarse siempre.

Esto evita que alguien entre a la red usando contraseñas robadas o dispositivos no autorizados.

🔗 Más información (NIST, gobierno de EE. UU.):
https://csrc.nist.gov/publications/detail/sp/800-207/final

---

2. Mantener vigilancia constante de la red

Así como un negocio usa cámaras, en tecnología también necesitamos "ver" lo que pasa.

En NetGuard Solutions recomendamos:

- Monitoreo 24/7.
- Alertas cuando algo se comporta diferente de lo normal.
- Revisión de actividades sospechosas.

🔗 SANS Institute – Buenas prácticas de monitoreo:
https://www.sans.org/white-papers/

🔗 CIS – Controles básicos de seguridad:
https://www.cisecurity.org/controls

---

3. Separar zonas dentro de la red

Lo explicamos a nuestros clientes así:
si una parte de la red se compromete, no debe arrastrar a toda la empresa.

Separar áreas críticas —como sistemas administrativos o información de clientes— hace la red mucho más segura.

🔗 Guía sencilla de CISA:
https://www.cisa.gov/resources-tools/resources/network-segmentation

---

4. Mantener los programas actualizados

Muchas amenazas entran porque un programa viejo tenía fallas conocidas.
Por eso insistimos en:

- Actualizar sistemas con regularidad.
- Aplicar parches de seguridad.
- Usar herramientas que automaticen estas tareas.

🔗 Informe de Verizon sobre causas comunes de ataques:
https://www.verizon.com/business/resources/reports/dbir/

🔗 CIS – Gestión de vulnerabilidades:
https://www.cisecurity.org/controls/vulnerabilities

---

5. Contraseñas seguras y verificación en dos pasos (MFA)

Una de las recomendaciones que más hacemos a nuestros clientes:

✔ Activar verificación doble (código por app o SMS).
✔ Cambiar contraseñas débiles.
✔ Revisar quién tiene acceso a qué áreas.

Esto evita que alguien entre usando una contraseña robada.

🔗 ISO 27001 – Control de acceso:
https://www.iso.org/standard/27001

---

6. Capacitar al personal

La seguridad no es solo tecnología: **las personas también deben saber cómo actuar**.

En NetGuard Solutions enseñamos a nuestros clientes a identificar:

- Correos falsos (phishing).
- Mensajes sospechosos.
- Archivos poco confiables.
- Errores comunes que pueden abrir la puerta a un ataque.

🔗 ENISA – Recursos de capacitación:
https://www.enisa.europa.eu/publications

---

7. Hacer copias de seguridad y tener un plan de emergencia

Los respaldos (backups) son indispensables.
Recomendamos:

- Copias automáticas frecuentes.
- Guardar algunas copias fuera de la red principal.
- Tener un plan claro sobre qué hacer si ocurre un ataque.

🔗 NIST – Marco de trabajo de ciberseguridad:
https://www.nist.gov/cyberframework

---

8. Revisar y auditar la seguridad con regularidad

Una empresa segura no lo es por casualidad. Necesita revisiones constantes.

Las auditorías ayudan a detectar fallas y corregirlas a tiempo.
En NetGuard Solutions hacemos este tipo de evaluaciones de manera continua para nuestros clientes.

🔗 ISACA – Guías de auditoría:
https://www.isaca.org/resources

Cómo te ayuda NetGuard Solutions

Además de compartir estas recomendaciones, en NetGuard Solutions apoyamos a nuestros clientes con herramientas diseñadas para que todo este trabajo sea más sencillo.

Nuestro software **NetGuard Pro** permite:

- Supervisar la red en tiempo real.
- Recibir alertas de actividad inusual.
- Organizar el tráfico para evitar saturaciones.
- Detectar comportamientos sospechosos.

Pero lo más importante: **acompañamos a cada empresa para que comprenda lo que ocurre en su red y pueda tomar decisiones informadas**.

Ingles

IT Security Best Practices for Businesses — A Simple Guide by NetGuard Solutions

At NetGuard Solutions, we work every day helping companies protect their networks. Many of our clients are not technology experts—and that's perfectly fine. **Our goal is to explain security in a way that is clear, friendly, and easy to understand.**

This guide shares the most important security practices recommended by international organizations, using simple language and including links so you can read more if you'd like.

---

1. Verify first, trust later (Zero Trust)

In security, the safest approach is:
don't automatically trust any device, user, or system—always verify.

This helps prevent unauthorized access, even if a password is stolen or a device is compromised.

🔗 Learn more (U.S. NIST official guide):
https://csrc.nist.gov/publications/detail/sp/800-207/final

---

2. Keep constant watch over your network

Just like a building has security cameras, your network also needs visibility.

At NetGuard Solutions, we recommend:

- 24/7 monitoring
- Alerts when something behaves differently
- Reviewing unusual or suspicious activity

This helps detect problems before they turn into serious incidents.

🔗 SANS Institute – Monitoring best practices:
https://www.sans.org/white-papers/

🔗 CIS Security Controls:
https://www.cisecurity.org/controls

---

3. Separate sensitive areas inside the network

We explain it to clients like this:
if one part of your network is affected, it should not put the entire company at risk.

Separating or isolating critical areas—such as administrative systems or customer data—greatly reduces your exposure.

🔗 CISA – Easy-to-understand network segmentation guidance:
https://www.cisa.gov/resources-tools/resources/network-segmentation

---

4. Keep software and systems updated

Many cyberattacks happen simply because a program was outdated.
Updating software is like changing the locks on your doors—old ones can be exploited.

We recommend:

- Regular updates
- Installing security patches
- Using tools that automate the update process

🔗 Verizon DBIR – Why attacks happen:
https://www.verizon.com/business/resources/reports/dbir/

🔗 CIS – Vulnerability management guidance:
https://www.cisecurity.org/controls/vulnerabilities

---

5. Use strong passwords and two-step verification (MFA)

One of the most important tips we share with customers is to use:

✔ Strong passwords
✔ Two-step verification (a code sent to your phone or app)
✔ Regular access reviews (who can access what)

This prevents many attacks caused by stolen passwords.

🔗 ISO 27001 – Access control standard:
https://www.iso.org/standard/27001

---

6. Train your team regularly

Security is not only about technology—**people play a huge role**.
Training helps your staff understand how to recognize and avoid threats, such as:

- Fake emails (phishing)
- Suspicious links or attachments
- Misleading messages
- Unsafe practices that open the door to attackers

🔗 ENISA – Cybersecurity training resources:
https://www.enisa.europa.eu/publications

---

7. Back up your data and have an emergency plan

Backups are like insurance—something you hope you never need, but you're very glad to have.

We recommend:

- Automatic, frequent backups
- Keeping some backups off the main network
- A clear plan on what to do in case of an attack

🔗 NIST Cybersecurity Framework:
https://www.nist.gov/cyberframework

---

8. Perform regular security reviews and audits

Just like a car needs maintenance, your security needs ongoing review.

Audits help identify weaknesses early and keep your security healthy.
At NetGuard Solutions, we help our customers run these evaluations regularly.

🔗 ISACA – IT audit guidelines:
https://www.isaca.org/resources

How NetGuard Solutions Supports You

Beyond sharing these best practices, our goal is to help businesses understand their networks clearly and make informed decisions.

Our software, **NetGuard Pro**, helps by:

- Monitoring your network in real time
- Sending alerts for unusual behavior
- Organizing traffic to prevent slowdowns
- Detecting suspicious or risky activity

Most importantly, **we guide each client step-by-step**, making security simple and manageable.