



Inspiring Technology
for People

CIBERSEGURIDAD PROACTIVA

Área de Seguridad
Fecha 01/04/2025
Versión 1.0

ÍNDICE DE CONTENIDOS

**La Evolución de las Ciberamenazas en
el Entorno Corporativo**

**Principales Amenazas para Empresas
Medianas y Grandes**

Estrategias de Seguridad Proactiva

**Implementación de un Plan de
Respuesta ante Incidentes (IRP)**

**La Importancia de la Capacitación
Continua para el Personal**

**Checklist para Evaluar el Nivel de
Seguridad de la Empresa**



Inspiring Technology
for People

LA EVOLUCIÓN DE LAS CIBERAMENAZAS

La ciberseguridad se ha convertido en un pilar fundamental en las organizaciones modernas, debido al creciente número de amenazas informáticas. La infraestructura corporativa se enfrenta a ataques cada vez más sofisticados, dirigidos y personalizados.

Incremento de Ataques Dirigidos: Antes los ciberdelicuentes solían lanzar ataques generales como correos de phishing o virus comunes, sin embargo ahora usan técnicas mas sofisticadas

Escasez de Talento en Ciberseguridad: A nivel mundial, hay pocas personas preparadas en ciberseguridad. Por ello pocas empresas pueden protegerse de manera escasa.

Dependencia Tecnológica: El uso de cada vez más tecnología hace que cada vez haya más puertas por donde un atacante podría entrar.

Principales Amenazas para Empresas

MEDIANAS Y GRANDES

Los ataques dirigidos son altamente sofisticados y **se centran en objetivos específicos dentro de la organización**. Emplean técnicas como el spear phishing, exploits de día cero y **suplantación de identidad**, aprovechando vulnerabilidades de software.

Fases de un **Ataque Dirigido**

Preparación: Recopilar información sobre la organización y empleados.

Infiltración: Uso de malware para ingresar sin ser detectado.

Exfiltración: Robo de datos sensibles y destrucción de evidencia.

EL RANSOMWARE MODERNO

Cifra grandes volúmenes de datos en poco tiempo y se propaga rápidamente en la red corporativa.

Características

Cifrado rápido y extendido: Bloquea datos en segundos.

Propagación lateral: Infecta dispositivos conectados.

Extorsión: Amenaza con divulgar datos si no se paga el rescate.

EL ATAQUE A LA MENTE HUMANA

Estos ataques explotan la psicología humana para obtener acceso a información sensible.

Técnicas comunes

Phishing: Correos fraudulentos que imitan fuentes confiables.

Vishing: Llamadas telefónicas engañosas.

Pretexting: Creación de historias falsas para obtener datos.

Estrategias de SEGURIDAD PROACTIVA

Endpoint Detection and Response (EDR)

Las soluciones EDR proporcionan un enfoque centralizado para la seguridad de los dispositivos conectados a la red.

Flujo de Trabajo de EDR

1. DETECCIÓN DE LA AMENAZA

El EDR monitorea en tiempo real el comportamiento de los dispositivos en busca de actividad sospechosa.

2. RESPUESTA AUTOMÁTICA

se toman acciones como aislar el dispositivo, bloquear procesos sospechosos o eliminar archivos maliciosos

3. ALERTA AL ADMINISTRADOR

Si la amenaza es significativa o requiere intervención manual, el EDR genera una alerta para el equipo de seguridad

4. REGISTRO FORENSE

Se registran todos los eventos clave como archivos ejecutados y esto permite rastrear el origen del ataque

5. ANÁLISIS DE LA CAUSA RAÍZ

Los analistas de seguridad revisan los datos recopilados para comprender como ocurrió la amenaza y prevenir futuros incidentes

Implementación de un **PLAN DE RESPUESTA ANTE INCIDENTES**

Un Plan de Respuesta ante Incidentes (IRP) es esencial para minimizar el impacto de cualquier ataque informático. La clave es contar con un plan detallado que esté listo para ser ejecutado en caso de un incidente de seguridad.

Componentes

- Preparación
- Detección y Análisis
- Contención y Erradicación
- Recuperación
- Lecciones Aprendidas

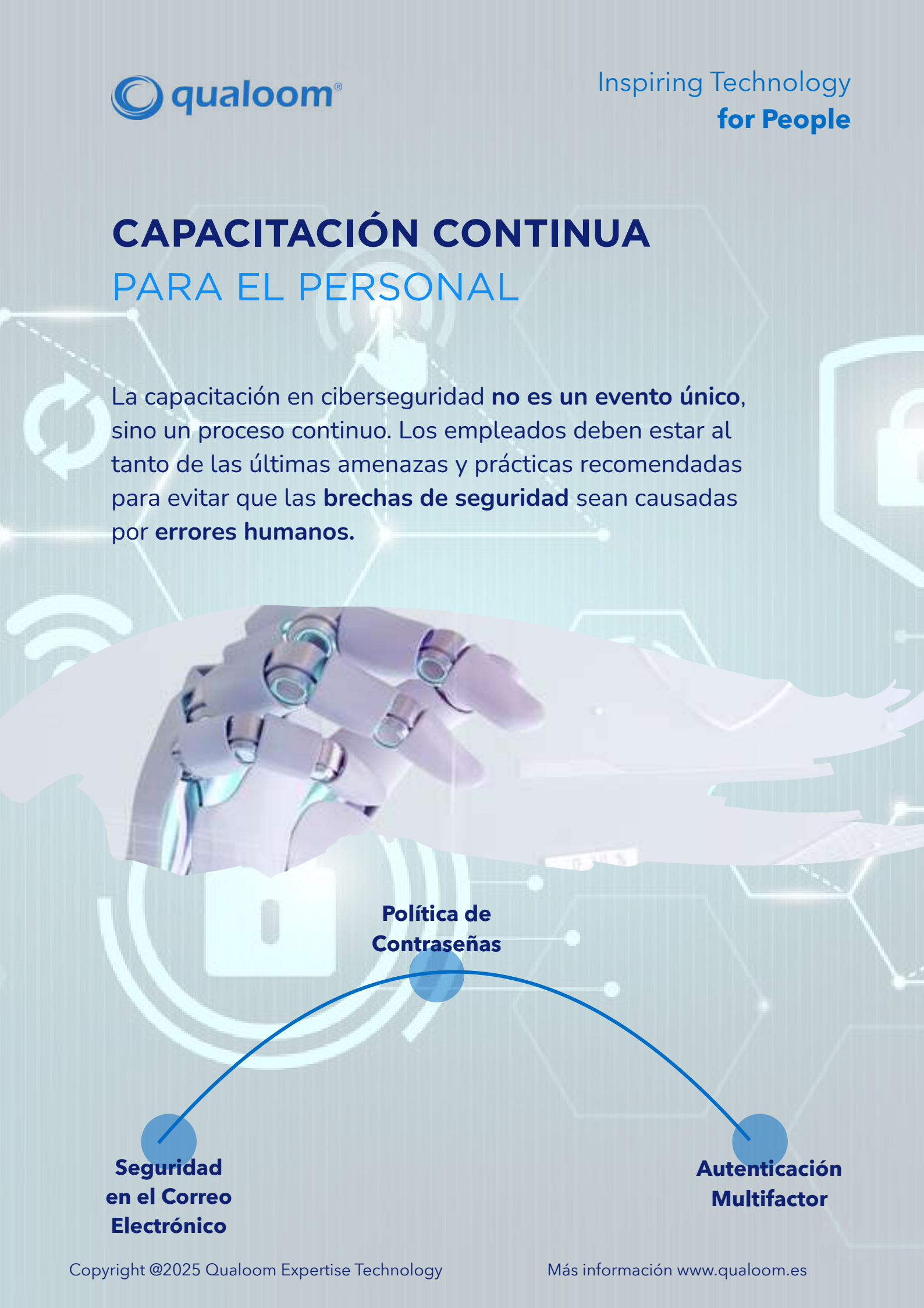


Ciclo de Respuesta

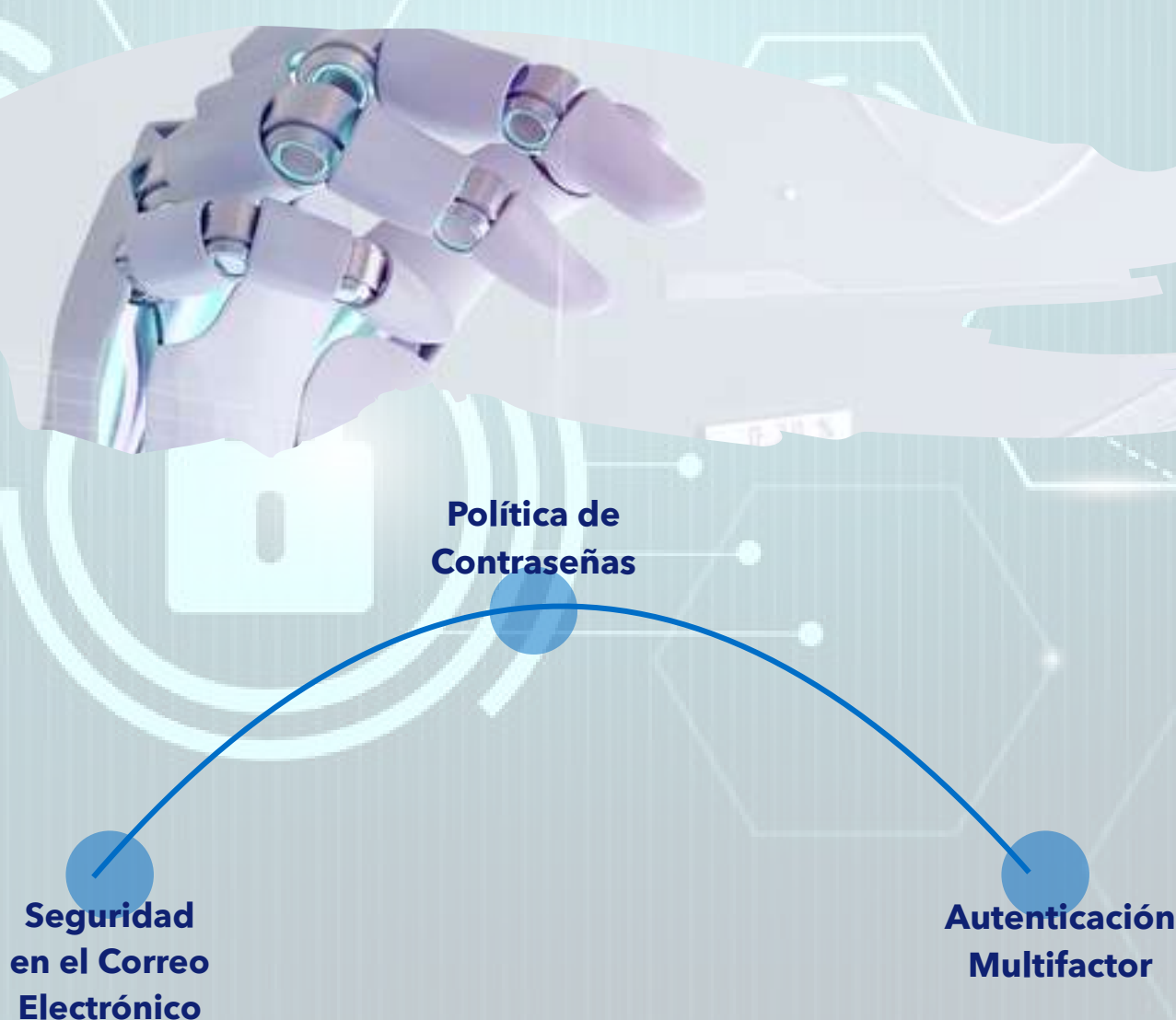


- Preparación
- Detección y Análisis
- Contención
- Erradicación
- Recuperación
- Lecciones Aprendidas

CAPACITACIÓN CONTINUA PARA EL PERSONAL



La capacitación en ciberseguridad **no es un evento único**, sino un proceso continuo. Los empleados deben estar al tanto de las últimas amenazas y prácticas recomendadas para evitar que las **brechas de seguridad** sean causadas por **errores humanos**.



**Seguridad
en el Correo
Electrónico**

**Política de
Contraseñas**

**Autenticación
Multifactor**

CHECKLIST

para **Evaluar el Nivel de Seguridad de la Empresa**

Para asegurar que la estrategia de ciberseguridad de la empresa es efectiva, es fundamental realizar auditorías periódicas y evaluaciones de seguridad.

Evaluación

¿Se realizan escaneos de vulnerabilidades con frecuencia?

¿Se usan firewalls y sistemas de detección de intrusos (IDS/IPS)?

¿Los datos críticos están cifrados tanto en reposo como en tránsito?

¿Existe un protocolo claro para la gestión de incidentes?

¿El personal tiene acceso solo a los datos que necesita?