

# Empresa más segura

en 20 sencillos pasos



EGUZKI

## Implementar Políticas de Seguridad Claras

Desarrollar, comunicar y hacer cumplir políticas de seguridad que abarquen todos los aspectos del uso de la tecnología y datos dentro de la empresa.

1

## Control de Acceso Basado en Roles (RBAC)

Limitar el acceso a recursos, sistemas y datos críticos únicamente a empleados que lo necesiten según su función específica en la organización.

2

## Autenticación Multifactor (MFA)

Requerir MFA para todas las cuentas críticas, reduciendo la posibilidad de acceso no autorizado incluso si las credenciales se ven comprometidas.

3

## Actualizaciones y Parches Regulares

Asegurar que todo el software y hardware se actualice regularmente con los últimos parches de seguridad para mitigar vulnerabilidades conocidas

4

## Cifrado de Datos

Implementar el cifrado tanto para datos en reposo como para datos en tránsito, protegiendo la información sensible contra accesos no autorizados.

5

## Copia de Seguridad Regular

Realizar y verificar copias de seguridad periódicas de datos críticos, y asegurarse de que las copias de seguridad estén almacenadas en lugares seguros, separados del entorno principal

6

## Segmentación de Redes

Dividir la red en segmentos más pequeños para aislar los sistemas críticos y reducir el riesgo de movimiento lateral por parte de los atacantes

7

## Firewalls y Sistemas de Detección de Intrusos (IDS/IPS)

Configurar y mantener firewalls y sistemas de detección y prevención de intrusos para monitorear y bloquear tráfico malicioso

8

## Protección contra Malware

Desplegar soluciones avanzadas de protección contra malware, como antivirus y software anti-ransomware, y mantenerlos actualizados.

9

## Concienciación y Formación de los Empleados

Realizar programas de formación y concienciación para empleados sobre amenazas comunes, como el phishing, y buenas prácticas de seguridad

10



# Empresa más segura

en 20 sencillos pasos

## Evaluaciones y Pruebas de Penetración

Realizar regularmente evaluaciones de vulnerabilidad y pruebas de penetración para identificar y corregir debilidades en la infraestructura de seguridad.

11



EGUZKI

## Gestión de Incidentes de Seguridad

Desarrollar, documentar y probar un plan de respuesta a incidentes de seguridad, asegurando una respuesta rápida y eficaz a cualquier brecha.

12

## Control de Dispositivos

Implementar políticas para el uso de dispositivos personales en la empresa (BYOD) y restringir el uso de dispositivos no autorizados para acceder a redes corporativas..

13

## Evaluación y Mitigación de Riesgos Regulares

Realizar evaluaciones periódicas de riesgos para identificar nuevas amenazas y ajustar las estrategias de seguridad en consecuencia.

14

## Seguridad en la Nube

Implementar controles de seguridad específicos para entornos en la nube, como la configuración adecuada de permisos, el cifrado de datos, y la utilización de herramientas de monitorización y respuesta ante incidentes para servicios en la nube.

15

## Auditorías de Seguridad

Realizar auditorías de seguridad internas y externas para verificar la eficacia de las políticas y controles de seguridad implementados.

16

## Gestión de Vulnerabilidades

Implementar un proceso formal para la identificación, priorización y remediación de vulnerabilidades en los sistemas y aplicaciones de la empresa.

17

## Monitoreo Continuo de Seguridad

Implementar soluciones de monitoreo continuo para detectar actividades sospechosas o anómalas en tiempo real y reaccionar rápidamente ante posibles amenazas.

18

## Gestión de Proveedores

Evaluar la seguridad de los proveedores externos y asegurarse de que cumplen con los estándares de seguridad necesarios, especialmente aquellos con acceso a datos sensibles.

19

## Redundancia y Recuperación ante Desastres

Desarrollar un plan de continuidad de negocio y recuperación ante desastres que asegure la capacidad de la empresa para recuperarse rápidamente de un incidente grave.

20