Empresa más segura

en 20 sencillos pasos

AUREA
ESCUELA TÉCNICA

1 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.

2 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.

3 Autenticación Multifactor (MFA)

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

4 Actualizaciones y Parches Regulares

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

5 Cifrado de Datos

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

6 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

7 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

8 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

9 Protección contra Malware

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

10 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

Empresa más segura

en 20 sencillos pasos

AUREA
ESCUELA TÉCNICA

11

Evaluaciones y Pruebas de Penetración

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

12

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.

13

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..

14

Evaluación y Mitigación de Riesgos Regulares

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

15

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.

16

Auditorías de Seguridad

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

17

Gestión de Vulnerabilidades

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

18

Monitoreo Continuo de Seguridad

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

19

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.

20

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.