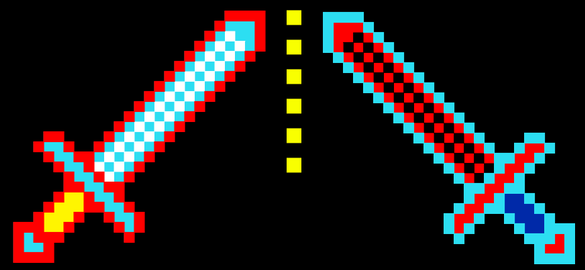
MANUAL SGSI - SISTEMA DE LA UNIVERSIDAD DE CALIFORNIA

¡¡ START !!



ALCANCE DEL SGSI

Activos identificados

- Hardware: servidores, equipos de red, computadoras personales.
- Software: sistemas académicos y administrativos.
- Datos: registros académicos, financieros y de investigación.

Límites virtuales

- Campus
- Centros de datos
- Áreas restringidas

Límites físicos

- Redes internas
- Entornos en la nube

EVALUACIÓN DE RIESGOS

Amenazas externas
Ransomware, phishing, desastres naturales.

Amenazas internas
Errores humanos, accesos indebidos.

Riesgos priorizados
Acceso no autorizado, malware, contraseñas débiles.

CONTROLES DE SEGURIDAD TÉCNICOS

- AUTENTICACIÓN MULTIFACTOR (MFA).
- CIFRADO DE DATOS SENSIBLES.
- FIREWALLS Y SISTEMAS DE DETECCIÓN DE INTRUSOS.
- ACTUALIZACIONES AUTOMATIZADAS.

CONTROLES DE SEGURIDAD ADMINISTRATIVOS Y FISICOS

- POLÍTICAS DE CONTRASEÑAS ROBUSTAS.
- AUDITORÍAS INTERNAS PERIÓDICAS.
- CONTROL DE ACCESO A INSTALACIONES CRÍTICAS.
- SISTEMAS DE VIDEOVIGILANCIA EN ÁREAS CLAVE.

POLÍTICAS Y PROCEDIMIENTOS

▪ PRINCIPIOS CLAVE

- Confidencialidad
- Integridad
- Disponibilidad

▪ RESPUESTA A INCIDENTES

- Identificación
- Notificación
- Contención
- Mitigación
- Cierre

▪ COPIAS DE SEGURIDAD

- Respaldos diarios/semanales
- Pruebas de recuperación

CAPACITACIÓN Y CONCIENCIACIÓN

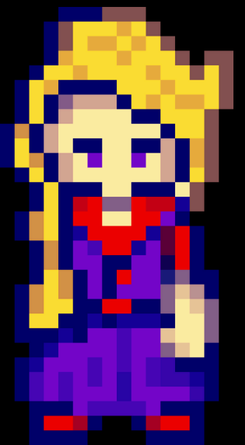
ANSWERS

A. Talleres iniciales para empleados

B. Talleres iniciales para estudiantes

C. Actualizaciones trimestrales sobre amenazas emergentes

D. Simulaciones de phishing y boletines informativos.



REVISIÓN Y APROBACIÓN

REVISIÓN ANUAL OBLIGATORIA.

REVISIONES EXTRAORDINARIAS TRAS INCIDENTES.

APROBACIÓN POR EL COMITÉ DE SEGURIDAD Y ADMINISTRACIÓN.

ÁREAS DE MEJORA

- AMPLIAR LA AUTOMATIZACIÓN EN ACTUALIZACIONES DE SISTEMAS.
- INCREMENTAR SIMULACIONES DE RESPUESTA A INCIDENTES.
- FORTALECER LA CAPACITACIÓN EN CIBERSEGURIDAD PARA EMPLEADOS.

PLAN DE MONITOREO CONTINUO

Indicadores clave (KPIs) • Reducción de incidentes de seguridad. • Disponibilidad superior al 99% para sistemas críticos.	Auditorías trimestrales y revisiones anuales.

MENU START SIGN IN

RESUMEN GENERAL

A. Alcance bien definido, con activos críticos identificados.

B. Amenazas y riesgos priorizados con controles adecuados.

C. Políticas y procedimientos alineados con estándares internacionales.

D. Capacitación y mejora continua como pilares del SGSI.

CONCLUSIÓN

El SGSI mejora la postura de seguridad de la Universidad de California.

Se mitigan riesgos críticos y se fomenta una cultura de ciberseguridad.

Planificación de monitoreo y revisiones periódicas garantizan su eficacia.