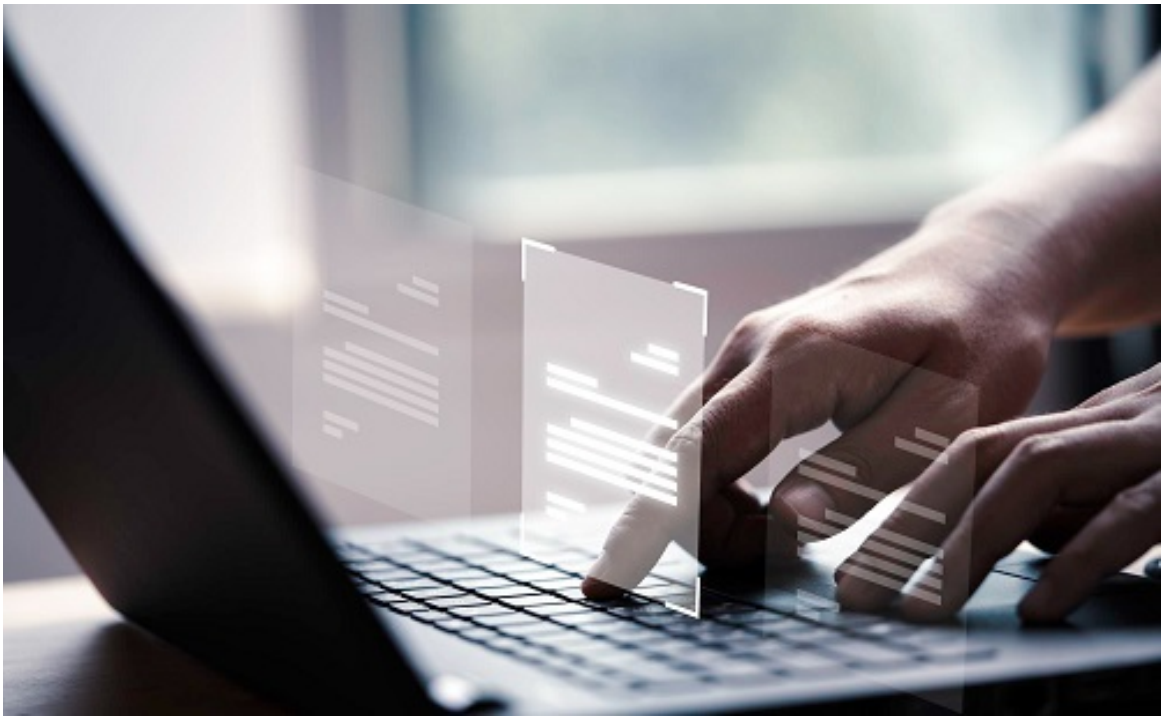
Actividad 1.1 Plan de concienciación



Trabajo realizado por:
Samuel Romero de los Reyes
Ernesto Saquete Ríos

Curso de especialización:
CETI

Índice

1. Definición de la empresa **2**
1.1. Estructura organizativa y departamentos 2
1.1.1. Departamento de Desarrollo y Producción (30 empleados) 2
1.1.2. Departamento de Administración y Marketing (15 empleados) 2
1.1.3. Equipos compartidos 3
1.1.4. Activos críticos 3
1.1.5. Infraestructura tecnológica 3
1.1.6. Posibles riesgos y amenazas 3
2. Plan de concienciación **4**
2.1. Análisis de riesgos 4
2.1.1. Amenazas técnicas 4
2.1.2. Amenazas humanas 4
2.1.3. Amenazas organizativas 5
2.2. Identificación de necesidades 5
2.3. Áreas y contenidos de formación 5
2.4. Grupos y roles implicados 6
2.5. Metodologías formativas 6
2.6. Programación del plan 7
2.7. Mantenimiento de la concienciación 7
2.8. Evaluación del plan 8

1. Definición de la empresa

Nombre de la empresa: Saquero Studios S.L.
Ámbito de negocio: Saquero Studios es una empresa española dedicada al desarrollo, publicación y distribución de videojuegos multiplataforma (PC, consolas y dispositivos móviles). Su principal objetivo es crear experiencias inmersivas con alto valor narrativo y artístico, combinando creatividad con innovación tecnológica. Además del desarrollo interno, la empresa ofrece servicios de diseño 3D y consultoría de gamificación para otras compañías del sector educativo y publicitario.

1.1. Estructura organizativa y departamentos

La empresa cuenta con dos sedes principales: una en Madrid (desarrollo y administración) y otra en Valencia (marketing y soporte técnico).
El total de empleados es de 45 personas, distribuidas en los siguientes departamentos principales:

1.1.1. Departamento de Desarrollo y Producción (30 empleados)

- Encargado del diseño, programación y testeo de los videojuegos.
- Cada programador y diseñador dispone de un PC de sobremesa de altas prestaciones (procesadores potentes y tarjetas gráficas dedicadas) para tareas de programación, modelado 3D y renderizado.
- Los diseñadores de sonido, guionistas y testers utilizan portátiles corporativos con acceso controlado al servidor de desarrollo mediante VPN.
- Los administradores de sistemas gestionan el servidor principal, que aloja los repositorios de código, las copias de seguridad y las herramientas de colaboración (Jira, GitHub Enterprise).
- El acceso al código fuente y a los entornos de prueba está restringido únicamente a este departamento.

1.1.2. Departamento de Administración y Marketing (15 empleados)

- El personal de contabilidad y recursos humanos utiliza PCs de sobremesa conectados a la red interna, con acceso limitado únicamente a los sistemas de gestión y documentos administrativos.
- Los responsables de marketing y community managers cuentan con portátiles para movilidad y gestión de campañas, además de smartphones corporativos (Android o iPhone) para redes sociales y comunicación con prensa o colaboradores externos.

- El equipo directivo dispone de portátiles y smartphones con acceso seguro a la nube y al servidor mediante autenticación multifactor (MFA).

1.1.3. Equipos compartidos

- Existen dos impresoras multifunción conectadas en red, accesibles únicamente desde las cuentas corporativas autenticadas.

- El servidor principal se encuentra en la sede de Madrid y gestiona las conexiones de ambos departamentos, con copia de respaldo automatizada.

- Algunos empleados del área de marketing pueden usar dispositivos personales bajo la política BYOD (Bring Your Own Device), siempre que instalen el software de seguridad corporativo y cumplan las políticas de protección de datos.

1.1.4. Activos críticos

- Código fuente de los videojuegos (repositorios Git internos y en la nube).

- Servidores de desarrollo y bases de datos de usuarios.

- Propiedad intelectual: diseños, música, guiones y modelos 3D.

- Equipos informáticos: PCs, portátiles, tablets gráficas y móviles corporativos.

- Datos personales de empleados y clientes.

- Cuenta bancaria y registros financieros.

1.1.5. Infraestructura tecnológica

La infraestructura tecnológica está compuesta por 35 PCs de sobremesa, 15 portátiles, varios dispositivos móviles corporativos y un servidor central en Madrid, todo bajo políticas de seguridad que incluyen autenticación multifactor, copias de seguridad automáticas y control de accesos.

1.1.6. Posibles riesgos y amenazas

Riesgos técnicos:

- Pérdida de código fuente o datos por fallo del servidor o malware.

- Ataques de ransomware o phishing dirigidos a empleados.

- Acceso no autorizado a sistemas internos o cuentas de almacenamiento en la nube.

Riesgos humanos:

- Fuga de información por descuido o empleados descontentos.
- Uso inadecuado de dispositivos personales (BYOD).
- Falta de formación en ciberseguridad básica.

Riesgos operativos:

- Interrupción del servicio por caídas de red o ataques DDoS.
- Pérdida de reputación por filtraciones o errores en comunicación.
- Incumplimiento de la normativa RGPD por mala gestión de datos personales.

2. Plan de concienciación

2.1. Análisis de riesgos

Tras el análisis previo de la infraestructura y los activos críticos de Saquero Studios S.L., se han identificado los principales puntos débiles que pueden comprometer la seguridad de la información y la continuidad del negocio:

2.1.1. Amenazas técnicas

- Infección por malware, ransomware o ataques de phishing dirigidos al personal de desarrollo y administración.
- Accesos no autorizados al servidor de desarrollo o a repositorios de código fuente.
- Pérdida o corrupción de información por fallos en el sistema de copias de seguridad.
- Uso inseguro de redes Wi-Fi o dispositivos personales (BYOD) sin las medidas de seguridad adecuadas.

2.1.2. Amenazas humanas

- Falta de concienciación del personal en materia de ciberseguridad.

- Manejo inadecuado de contraseñas o reutilización en servicios externos.
- Divulgación involuntaria de información sensible o propiedad intelectual.
- Ausencia de procedimientos claros ante incidentes de seguridad.

2.1.3. Amenazas organizativas

- Escaso control sobre la gestión documental impresa o compartida.
- Comunicación deficiente entre departamentos respecto a prácticas seguras.
- Pérdida de reputación por filtración o mal uso de datos de usuarios.

2.2. Identificación de necesidades

Las necesidades de formación detectadas se centran en los siguientes ámbitos:

- Personal técnico (programadores, diseñadores, testers): deben reforzar el uso seguro de repositorios, contraseñas y herramientas colaborativas.
- Personal administrativo y de marketing: necesitan concienciación en el tratamiento de datos personales, seguridad en el correo electrónico y prevención del phishing.
- Dirección y mandos intermedios: requieren conocimientos sobre gestión de incidentes, cumplimiento del RGPD y supervisión de políticas internas.
- Toda la plantilla: debe asimilar buenas prácticas en el uso del puesto de trabajo, redes, dispositivos y contraseñas.

El objetivo general es crear una cultura de seguridad transversal que abarque tanto el entorno laboral como los hábitos digitales personales.

2.3. Áreas y contenidos de formación

Área de formación	Contenidos principales	Objetivo
Gestión de contraseñas y autentificación	Contraseñas seguras, MFA, gestores de contraseñas	Prevenir accesos no autorizados
Ingeniería social y phishing	Reconocimiento de correos falsos, webs fraudulentas, suplantación de identidad	Evitar engaños que comprometan datos o sistemas
Protección de la información	Clasificación de datos, copias de seguridad, confidencialidad	Asegurar la integridad y disponibilidad de la información

Uso seguro del puesto de trabajo	Bloqueo de pantalla, documentos impresos, entorno físico seguro	Minimizar fugas o exposiciones accidentales
Dispositivos y movilidad	Cifrado, uso de VPN, políticas BYOD, custodia de equipos	Garantizar la seguridad fuera de la oficina
Cumplimiento normativo	RGPD, propiedad intelectual, uso legítimo de software	Cumplir la legislación vigente y políticas internas

2.4. Grupos y roles implicados

Grupo/Rol	**Formación específica**	**Responsable/Formador**
Programadores y diseñadores	Seguridad en repositorios Git, uso de VPN y MFA	Administrador de sistemas
Testers y QA	Protección de datos en entornos de prueba, gestión de incidentes	Coordinador de desarrollo
Administración y RRHH	Gestión de datos personales, correos seguros	Responsable de seguridad y DPO externo
Marketing y Community Managers	Seguridad en redes sociales y dispositivos móviles	Departamento IT / Comunicación
Dirección y mandos	Supervisión del plan, políticas de seguridad, respuesta ante incidentes	Responsable de sistemas
Toda la plantilla	Buenas prácticas generales, campañas periódicas	Coordinador del plan

2.5. Metodologías formativas

El plan combinará formación teórica y práctica, con materiales dinámicos y de fácil comprensión:

- Píldoras formativas de 10-15 minutos sobre temas clave (contraseñas, phishing, redes sociales, RGPD).
- Charlas presenciales o videoconferencias trimestrales impartidas por el responsable de seguridad.

- Cartelería y mensajes visuales en zonas comunes y pantallas corporativas.
- Correos informativos con ejemplos de amenazas reales.
- Simulacros de phishing trimestrales para evaluar la concienciación.
- Portal interno con materiales descargables y vídeos de buenas prácticas.

2.6. Programación del plan

El plan inicial tendrá una duración de 6 meses, repitiéndose anualmente con actualizaciones.

Fase	Periodo	Actividades principales
I - Lanzamiento	Semana 1-2	Presentación del plan y primera charla general
II - Formación base	Mes 1-2	Píldoras formativas sobre contraseñas y phishing
III - Seguridad en el puesto de trabajo	Mes 3	Campaña visual “Tu mesa también guarda secretos”
IV - Movilidad y BYOD	Mes 4	Taller práctico sobre VPN y seguridad móvil
V - Refuerzo y evaluación	Mes 5-6	Simulacro de phishing, encuesta y análisis de resultados

2.7. Mantenimiento de la concienciación

Para garantizar la continuidad del aprendizaje y mantener el interés de los empleados se aplicarán las siguientes medidas:

- Enviar boletines mensuales con novedades de ciberseguridad.
- Incorporar una sesión introductoria de seguridad en la acogida de nuevos empleados.
- Actualizar la cartelería interna cada trimestre con mensajes distintos.
- Reforzar las campañas en fechas clave (Navidad, vacaciones, lanzamientos de productos).
- Realizar pruebas de respuesta a incidentes anuales.
- Evaluar y actualizar las políticas BYOD y contraseñas cada 12 meses.

2.8. Evaluación del plan

Se establecerán indicadores y métodos de evaluación para medir la eficacia del programa:

Elemento a auditar	Modo de evaluación	Frecuencia
Uso de contraseñas seguras	Revisión de políticas y registros de autenticación	Semestral
Phishing y correos sospechosos	Simulaciones y análisis de respuestas	Trimestral
Documentos impresos	Inspección aleatoria de bandejas de impresoras	Mensual
Cumplimiento de políticas BYOD	Revisión del software de seguridad instalado	Semestral
Participación en formaciones	Registro de asistencia y test online	Al finalizar cada sesión

Los resultados serán revisados por el responsable de sistemas y comunicados a la dirección para definir mejoras y nuevas acciones.