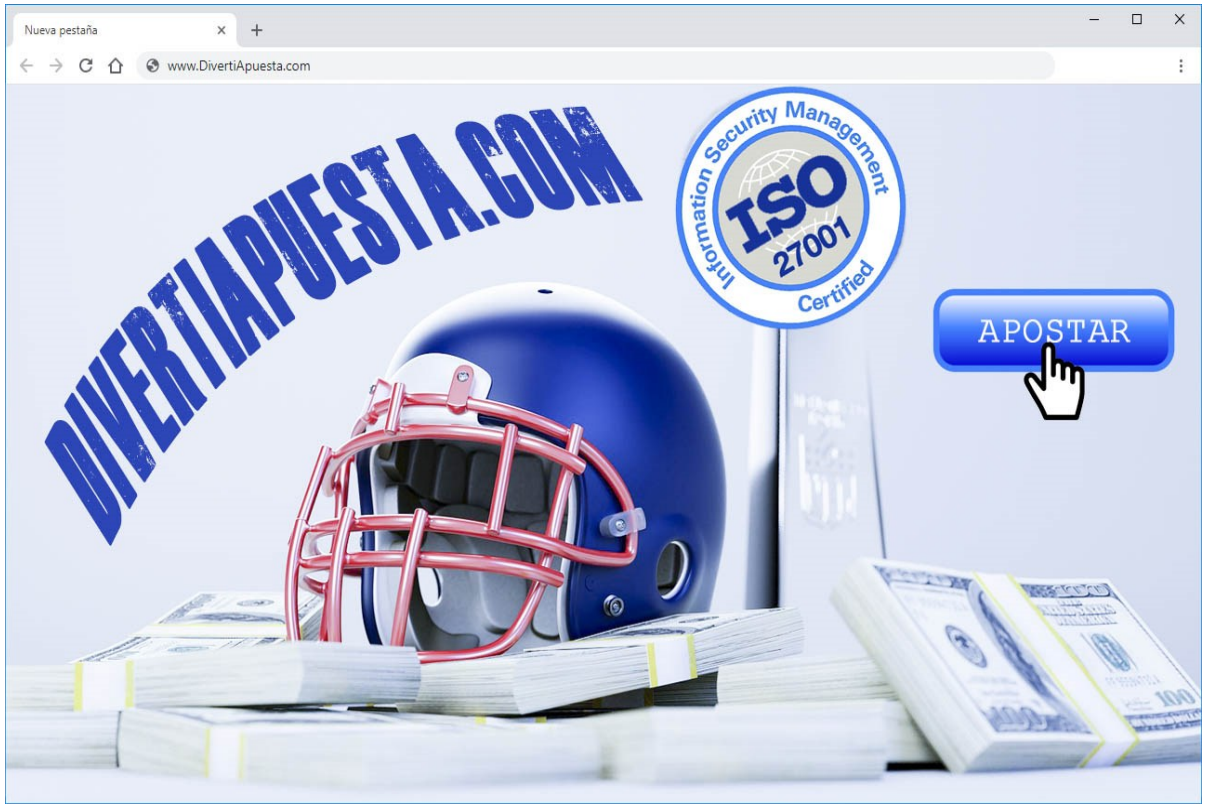
Adecuación ISO 27001
Presentación a dirección



Adrián Capdevila

Máster Universitario en
Seguridad de las TIC - MISTIC

Objetivo

Análisis del proyecto de adecuación + concienciación

Contenido:

- La seguridad de la información y DivertiApuesta
- Amenazas y salvaguardas
- Motivos para la implantación
- Mejoras esperadas

La seguridad de la información y DivertiApuesta

El 100% del volumen de negocio de DivertiApuesta se basa en tecnologías de la información:

- No creamos o comerciamos con productos físicos.
- No ofrecemos servicios que no dependan de TI.
- No tenemos otra actividad aparte del juego online/telemático.
- No tenemos una patente sobre un producto que solo nosotros conozcamos.
- Sin perdemos los datos de nuestros clientes, los perdemos.
- Si cae la plataforma, la competencia está a un solo clic.
- Si dejamos de ser competitivos o confiables, perdemos patrocinadores.

La seguridad de la información y DivertiApuesta

TODO nuestro negocio depende de nuestros servidores, nuestra información, nuestros conocimientos y la confianza de nuestros usuarios…

... y todo puede desaparecer en minutos por un solo error.

Don’t panic yet

DivertiApuesta cuenta con sistemas de seguridad avanzados y personal encargado de mitigar las amenazas, pero la seguridad de la información es cosa de todos: es una cadena que siempre romperá por el eslabón más débil

Amenazas y salvaguardas

Amenazas Principales	Salvaguardas
Errores Humanos: • Por falta de control • Por falta de conocimientos • Por falta de atención o esmero	• Desarrollo de procedimientos • Gestión controlada de los sistemas • Formación y concienciación • Dimensionamiento adecuado de departamentos y carga de trabajo • Copias de seguridad
Ataques informáticos: • Phishing • Malware (navegación, USB, correo electrónico, etc) • Equipos vulnerables	• Formación y concienciación. • Medidas técnicas antimalware (antivirus gestionado, IPS, copias de seguridad, etc) • Gestión controlada de los sistemas • Revisiones periódicas de seguridad • Copias de seguridad
Incidencias fortuitas: • Averías físicas • Software o hardware deficiente • Fallo de proveedores	• Equipos y planes de respaldo • Copias de seguridad • Mantenimiento adecuado de SW y HW
Incumplimientos legales	Gestión, control y auditorías de cumplimiento

Debilidades Fortalezas Amenazas y Oportunidades ACTUALES

DEBILIDADES

- Alta dependencia tecnológica
- Sin gestión formal de la seguridad
- Seguridad poco escalable

FORTALEZAS

- Personal muy competente
- Importante cartera de usuarios
- Pocas incidencias en el servicio

AMENAZAS

- Indisponibilidad del servicio por motivos de seguridad
- Daño reputacional por hackeo
- Impacto enorme por fallos puntuales

OPORTUNIDADES

- Posicionarse como plataforma de confianza.
- Atraer inversiones por nuestra fiabilidad

Debilidades Fortalezas Amenazas y Oportunidades FUTURAS

DEBILIDADES

- Alta dependencia tecnológica (se mantiene)
- Gestión la seguridad mejorada
- Seguridad más escalable

FORTALEZAS

- Refuerzo de la capacitación
- Mejoraremos confianza de los usuarios
- Reduciremos más las incidencias en el servicio

AMENAZAS

- Menos indisponibilidad del servicio por seguridad
- Probabilidad de hackeo reducida
- Menos impacto por fallos

OPORTUNIDADES

- Ventaja competitiva contra la competencia
- Generaremos más confianza en posibles inversores

Mejoras esperadas

- Se aumentará el nivel de concienciación sobre ciberseguridad
- Se ha establecerá la hoja de ruta para la evolución de la seguridad
- Se optimizarán los recursos dedicados a tareas de seguridad
- Facilitará el crecimiento escalable de la organización sin comprometer los sistemas y seguridad
- Se reducirán significativamente los riesgos de pérdidas económicas por incidentes de seguridad
- Se dispondrá de una plataforma tecnológica más tolerante a fallos