Auditoría NIST SP 800-53, Ebury

Introducción

Ebury es una plataforma financiera que ofrece servicios de pagos, cobros, riesgo cambiario y financiación para empresas que operan a nivel global. Debido a la naturaleza de sus servicios, está sujeta a estrictos requisitos de ciberseguridad, incluyendo la protección de datos financieros sensibles y el cumplimiento de normativas internacionales. Se llevará a cabo una auditoría basada en el marco de control de seguridad NIST SP 800-53, que es un estándar utilizado para implementar medidas de seguridad de la información.

Objetivo

El objetivo de la auditoría es asegurar que Ebury esté alineada con las mejores prácticas de ciberseguridad y cumpla con los requisitos de NIST SP 800-53 para la protección de los activos y la información crítica, minimizando el riesgo de amenazas cibernéticas.

Alcance de la Auditoría

La auditoría abarcará las áreas clave de seguridad que establece NIST SP 800-53. Esto incluye la revisión de controles de seguridad organizacionales, técnicos y operacionales en Ebury.

Las áreas a evaluar incluyen:

1. **Controles de Acceso (AC)**
2. **Conciencia y Capacitación de Seguridad (AT)**
3. **Auditoría y Responsabilidad (AU)**
4. **Protección de Sistemas de Información (SC)**
5. **Mantenimiento de Seguridad (MA)**
6. **Gestión de Incidentes (IR)**
7. **Planificación de Contingencias (CP)**
8. **Autenticación y Autorización (IA)**

1. Controles de Acceso (AC)

Objetivo: Evaluar cómo Ebury gestiona el acceso a sistemas y datos críticos, asegurando que solo los usuarios autorizados tienen acceso adecuado. Esto incluye tanto accesos físicos como lógicos a los sistemas.

Control	Descripción del Control	Hallazgo	Nivel de Cumplimiento (1-5)	Recomendación	Pregunta realizada	Responsable/ Departamento
AC-2: Control de Acceso Basado en Roles (RBAC)	Los usuarios solo deben tener acceso a los recursos necesarios para su función.	Algunos usuarios tienen privilegios excesivos para sus funciones.	3	Implementar una revisión automatizada periódica de los permisos para garantizar que solo se otorguen accesos mínimos necesarios.	¿Cómo está gestionado el acceso basado en roles y los privilegios dentro de los sistemas críticos?	Responsable de IT y Ciberseguridad
AC-3: Gestión de Acceso a Recursos Críticos	Control estricto del acceso a sistemas financieros y sensibles.	El acceso a sistemas financieros está controlado, pero se detectaron cuentas compartidas en algunos sistemas.	2	Eliminar el uso de cuentas compartidas e implementar acceso individualizado y rastreable para todos los sistemas.	¿Se revisan periódicamente los accesos de los usuarios para detectar posibles excesos de privilegios?	Responsable de IT
AC-5: Separación de Funciones	Garantizar que las funciones críticas estén separadas entre diferentes usuarios.	Algunas funciones administrativas y operativas están combinadas en un solo usuario.	3	Implementar la separación total de funciones críticas entre usuarios diferentes para mitigar el riesgo de abuso de poder o negligencia.	¿Están separadas las funciones críticas entre diferentes usuarios o roles para evitar conflictos de interés?	Jefe de Operaciones y IT
AC-6: Supervisión del Acceso	Supervisión activa de los accesos para detectar y mitigar accesos no autorizados.	No existe un sistema de alertas automático para accesos sospechosos.	2	Implementar un sistema de alertas automáticas en tiempo real para accesos sospechosos o anómalos en sistemas críticos.	¿Existe un mecanismo para monitorear los accesos sospechosos o no autorizados a los sistemas?	Departamento de Seguridad Informática

2. Conciencia y Capacitación de Seguridad (AT)

Objetivo: Garantizar que el personal de Ebury esté capacitado en ciberseguridad y pueda identificar y mitigar riesgos básicos como phishing, ingeniería social, etc.

Control	Descripción del Control	Hallazgo	Nivel de Cumplimiento (1-5)	Recomendación	Pregunta realizada	Responsa Departan
AT-2: Capacitación en Seguridad de la Información	Establecer un programa de capacitación de seguridad continuo para todo el personal.	El índice de asistencia al entrenamiento de ciberseguridad es solo del 75%, por debajo del umbral del 95%.	3	Incrementar la frecuencia de las capacitaciones y realizar simulacros trimestrales para mantener a los empleados actualizados.	¿Qué programa de capacitación de ciberseguridad tienen implementado para el personal?	Departame de Recurso Humanos Seguridad
AT-3: Actualización de Conocimientos de Seguridad	Proporcionar actualizaciones regulares sobre las amenazas y vulnerabilidades emergentes.	No se hacen capacitaciones específicas sobre nuevas amenazas emergentes, como fraudes financieros.	2	Implementar una capacitación especializada en amenazas emergentes, con foco en ataques de ingeniería social y fraudes financieros.	¿Con qué frecuencia actualizan a los empleados sobre nuevas amenazas de ciberseguridad, como ataques de ingeniería social o phishing?	Departame de Cibersegu

3. Auditoría y Responsabilidad (AU)

Objetivo: Evaluar los mecanismos de registro y monitoreo de eventos de seguridad, asegurando que se mantienen auditorías efectivas.

Control	Descripción del Control	Hallazgo	Nivel de Cumplimiento (1-5)	Recomendación	Pregunta realizada	Responsable/ Departamento
AU-2: Registro de Eventos de Seguridad	Se deben registrar todos los eventos críticos relacionados con la seguridad.	Se registran eventos, pero la retención de logs es de solo 12 meses y no hay alertas automáticas.	3	Extender la retención de logs a 24 meses y configurar alertas automáticas para accesos no autorizados.	¿Cuánto tiempo se almacenan los registros de eventos de seguridad y cómo se asegura la integridad de estos logs?	Responsable de Auditoría y Departamento de IT
AU-6: Monitoreo y Análisis de Eventos de Seguridad	Monitorear y analizar regularmente los eventos de seguridad registrados.	Los logs se recopilan, pero no se realiza un análisis regular ni automatizado de los eventos.	2	Automatizar el análisis de logs y usar herramientas de detección de anomalías para monitorear posibles incidentes en tiempo real.	¿Qué mecanismos de análisis y monitoreo se utilizan para detectar incidentes a partir de los eventos de seguridad registrados?	Departamento de Seguridad Informática

4. Protección de Sistemas de Información (SC)

Objetivo: Asegurar que los sistemas críticos de Ebury están protegidos frente a amenazas internas y externas, como accesos no autorizados, malware, etc.

Control	Descripción del Control	Hallazgo	Nivel de Cumplimiento (1-5)	Recomendación	Pregunta realizada	Resp Depa
SC-8: Protección de Datos en Tránsito	Implementar cifrado para proteger los datos mientras están en tránsito.	El cifrado está implementado para datos en tránsito, pero no se han revisado sus configuraciones en los últimos 12 meses.	4	Revisar periódicamente las configuraciones de cifrado y asegurarse de que cumplan con los estándares de seguridad actuales.	¿Qué tipo de cifrado se utiliza para proteger los datos en tránsito y con qué frecuencia se revisan las configuraciones ?	Respo IT
SC-12: Parcheo de Vulnerabilidades	Aplicar parches en tiempo oportuno para corregir vulnerabilidades de seguridad críticas.	Los parches de vulnerabilidades críticas tardan más de 30 días en ser aplicados.	2	Reducir el tiempo de parcheo a un máximo de 7 días para vulnerabilidades críticas.	¿Qué protocolo siguen para aplicar parches de seguridad críticos y cuál es el tiempo medio para implementar estos parches?	Jefe d Segur y Dep de IT