Diseño de Contramedidas
Cuestionario Realizado (Evaluar modelo de madurez – Generar Contramedidas NIST SP 800-53)

Encuesta basada en auditores PWC

Identify

ID.AM-4: Inventario de Activos: Este control implica la identificación y mantenimiento de un inventario de todos los activos de información relevantes para la entidad financiera. Esto incluye tanto los activos digitales (como sistemas, bases de datos y aplicaciones) como los activos físicos (como dispositivos de hardware y medios de almacenamiento).

ID-RA-5: Análisis de Riesgos: Este control establece la realización de análisis de riesgos periódicos para identificar y evaluar las amenazas, vulnerabilidades y posibles impactos en los activos de información de la entidad financiera. Estos análisis son fundamentales para comprender las amenazas y riesgos a los que se enfrenta la organización.

ID.BE-1: Política de Gestión de Identidad y Acceso: Este control implica el desarrollo e implementación de políticas y procedimientos para la gestión de identidades y accesos dentro de la entidad financiera. Esto incluye la asignación de roles y privilegios apropiados, la autenticación de usuarios y la protección de credenciales de acceso.

ID.AN-1: Análisis de Impacto en el Negocio: Este control establece la realización de análisis de impacto en el negocio para identificar y evaluar las consecuencias potenciales de interrupciones en los servicios y operaciones de la entidad financiera. Este análisis ayuda a priorizar la protección de los activos críticos para el negocio.

ID.AM-4: Actualización del Inventario de Activos: Este control establece procesos y procedimientos para garantizar que el inventario de activos de la entidad financiera se mantenga actualizado y sea relevante en todo momento. Esto incluye la incorporación de nuevos activos, así como la eliminación de activos obsoletos o retirados.

Protect

PL-4: Protección contra Ataques Conocidos: Este control implica el uso de medidas de seguridad, como firewalls, sistemas de detección de intrusos y filtrado de

contenido, para proteger contra ataques conocidos. Estas medidas ayudan a prevenir y mitigar los efectos de intrusiones maliciosas y actividades no autorizadas.

SI-4: Monitoreo de Seguridad: Este control establece la implementación de sistemas y procesos para monitorear continuamente la seguridad de la información y los sistemas. El monitoreo constante permite detectar y responder de manera oportuna a posibles amenazas y vulnerabilidades.

SA-11: Sesiones de Administración Remota encriptadas: Dado que las entidades financieras manejan datos sensibles, este control es crucial. Establece que las sesiones de administración remota, como el acceso a sistemas desde ubicaciones externas, deben estar encriptadas para proteger la confidencialidad e integridad de la información.

Detect

SI-4 Monitoreo de Seguridad: Este control implica la implementación de sistemas y procesos para monitorear continuamente la seguridad de la información y los sistemas. El monitoreo constante permite detectar y responder de manera oportuna a posibles amenazas y vulnerabilidades.

SI-7 Monitoreo de Seguridad Continuo: Similar al anterior, este control establece la implementación de sistemas de monitoreo continuo para detectar y responder a eventos de seguridad en tiempo real. El monitoreo continuo es esencial para identificar y mitigar amenazas en evolución de manera oportuna.

SI-3 Análisis de Seguridad de la Información: Este control implica la realización de análisis periódicos de la seguridad de la información para identificar y evaluar las vulnerabilidades y riesgos de seguridad. Estos análisis ayudan a comprender mejor el panorama de seguridad y a priorizar las acciones de mitigación.

SI-5 Reporte de Incidentes: Este control establece procesos y procedimientos para la detección, notificación y respuesta a incidentes de seguridad de la información. Una respuesta rápida y eficiente a incidentes es fundamental para minimizar el impacto de posibles amenazas cibernéticas.

SI-7(d) Alertas Automatizadas: Este control implica la implementación de alertas automáticas que notifican al personal de seguridad sobre eventos de seguridad importantes. Las alertas automatizadas permiten una respuesta rápida a posibles amenazas y ayudan a garantizar que se tomen medidas de mitigación adecuadas de manera oportuna.

Respond

R-4 Reporte de Incidentes: Este control establece procesos y procedimientos para la detección, notificación y respuesta a incidentes de seguridad de la información. Una respuesta rápida y eficiente a incidentes es fundamental para minimizar el impacto de posibles amenazas cibernéticas.

CP-2 Plan de Continuidad del Negocio: Este control implica la elaboración y mantenimiento de un plan de continuidad del negocio que establezca los procedimientos y recursos necesarios para mantener las operaciones críticas durante y después de un incidente de seguridad. Este plan garantiza que la entidad financiera pueda seguir funcionando incluso en situaciones adversas.

IR-8 Entrenamiento del Equipo de Respuesta a Incidentes: Este control establece la realización de entrenamientos y ejercicios regulares para el equipo de respuesta a incidentes, con el fin de asegurar que estén preparados para enfrentar eficazmente posibles incidentes de seguridad. El entrenamiento constante es esencial para mantener al equipo actualizado sobre las mejores prácticas y procedimientos de respuesta.

IR-10 Análisis Posterior al Incidente: Este control implica la realización de un análisis exhaustivo después de cada incidente de seguridad para identificar las causas raíz, evaluar el impacto y determinar las medidas correctivas necesarias para prevenir futuros incidentes similares. El análisis posterior al incidente es crucial para mejorar continuamente la postura de seguridad de la entidad financiera.

CP-4 Pruebas del Plan de Continuidad del Negocio: Este control establece la realización periódica de pruebas y ejercicios para evaluar la eficacia del plan de continuidad del negocio y garantizar su capacidad para mantener las operaciones críticas en caso de un incidente de seguridad. Las pruebas del plan son fundamentales para identificar y abordar cualquier debilidad o área de mejora en el plan de continuidad.