Gestión Integral de Riesgos

Nombre del documento:	**Metodología de evaluación del riesgo de los activos**		
Tipo:	Metodología del riesgo integral	**Documento #:**	1
Propietario del documento:	Luis Bustamante, BISO Security LATAM	**Emitido por:**	Luis Bustamante
Aprobado por:	Junta Directiva	**Fecha de la última revisión:**	03/04/2022
Fecha de entrada en vigor:	03/04/2022	**Próxima fecha de revisión:**	03/04/2022

Índice de contenidos

1. Introducción…….3

2. Alcance…….3

2.1. Definiciones……...3

2.2. Organigrama……..4

2.3. Representantes……4

2.4. Responsabilidad de los empleados……...5

2.5. Definiciones……5

3. Identificación de riesgos……..5

3.1. Calificación de riesgo inherente(IRR) 5

3.2 Cálculo de la calificación de riesgo inherente (IRR).....6

4. Análisis de riesgos…...……..9

4.1. Clasificación de la evaluación del control(CAR) 9

4.2. Cálculo del índice de evaluación del control (CAR)Cálculo.....10

5. Evaluación de riesgos……

……10

5.1. Calificación de riesgo residual.....10

5.2. Cálculo de la calificación de riesgo 11

5.3. Resultados de la evaluación de 11

6. Tratamiento del riesgo…… ……..11

7. Control de riesgos…… ……13

1.Introducción

La Metodología de Evaluación de Riesgos definida en este documento se utiliza a lo largo del ciclo de vida de la evaluación de riesgos para priorizar los activos de Equifax en función de los riesgos. El resultado de la evaluación de riesgos permite a los líderes de negocio y a las partes interesadas tomar decisiones informadas sobre el riesgo, proporcionando un análisis objetivo de los riesgos que pueden afectar a Equifax. El ciclo de vida de la evaluación de riesgos se describe en los siguientes pasos:

- **Identificación de riesgos**: Identificar y priorizar los activos de Equifax en función de los atributos de riesgo inherentes.
  - Calificación de riesgo inherente (IRR)
- **Análisis de riesgos**: Analizar la eficacia operativa de los principales controles de Equifax.
  - Clasificación de la evaluación del control (CAR)
- **Evaluación del riesgo**: Evaluar el riesgo residual que queda después de valorar la eficacia del control.

- Calificación de riesgo residual (RRR)

• **Tratamiento del riesgo**: Determinar la calificación de las deficiencias de control identificadas a través del proceso de evaluación de riesgos.

- Calificación del impacto de la emisión (IIR)

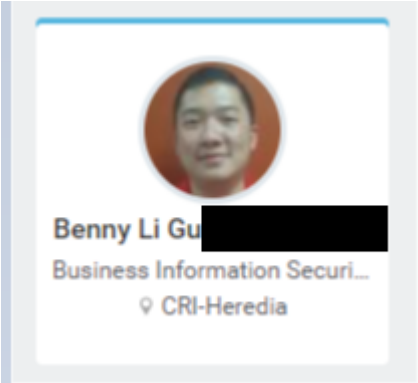
• **Seguimiento de los riesgos**: Supervisar los activos según la cadencia del riesgo. ○ Calendario de reevaluación

2. Alcance

Este documento describe la metodología de riesgos para de Equifax. Esto incluye: definiciones, la calificación de riesgo inherente, la calificación de evaluación de control, la calificación de riesgo residual, la calificación de impacto de los problemas y la cadencia de las actividades de reevaluación.

2.1. Organigrama

Los responsables de liderar todos los comités de gestión de riesgo para monitorear todos los riesgos identificados



2.2. Representantes

- Douglas Sánchez - Managing Director
- Juan Lecaros - International Operations Senior Manager
- Ever Espinoza - Software Engineer Senior Manager
- Luis Bustamante - BISO CAMEX
- Rebeca Fernandez - Legal Counsel
- Benny Li Gu - Business Information Security Officer

2.3. Periodicidad y descripción de las herramientas a utilizar para la gestión del riesgo

Los comité de riesgo se llevarán a cabo de manera mensual, utilizando la información y herramientas

que el área de Issues Management nos provee para monitorear los diferentes riesgos.

2.4. Responsabilidad de los empleados

Todos los involucrados en el proceso de gestión de riesgos deberán participar en todo el ciclo,de identificación, verificación, análisis, remediación y monitoreo de los riesgos con el objetivo de mitigar todos los riesgos e incidentes identificados y así minimizar su exposición de la compañía.

2.5. Definiciones

- **Activo**: Se refiere a las aplicaciones y plataformas de Equifax utilizadas para realizar un proceso de negocio o un componente del mismo.
    - **Aplicaciones**: incluye programas de software, formularios, scripts, flujos de trabajo o una colección de ellos.
    - **Plataformas**: incluye las tecnologías o infraestructuras subyacentes.
- **Riesgo inherente**: Se refiere al nivel de riesgo sin la consideración de los controles.
- **Control**: Se refiere a una actividad técnica y/o administrativa destinada a reducir el riesgo.
- **Eficacia del control**: Se refiere a la eficacia operativa de un control que mitiga el riesgo.
- **Riesgo residual**: Se refiere al nivel de riesgo que queda después de contabilizar los controles.

3. Identificación de riesgos

3.1. Calificación de riesgo inherente (IRR)

El primer paso en el ciclo de vida de la evaluación de riesgos es determinar la TIR de cada activo. La TIR se utiliza para priorizar la criticidad de los activos de Equifax.

Las calificaciones de la TIR se definen a continuación:

- **Crítico:** Activos de los que Equifax depende en gran medida en el desempeño de un proceso de negocio o componente de donde podría haber un impacto severo a través de la pérdida o corrupción de datos de Equifax. Cualquier interrupción, fallo o falta de control podría tener un impacto inmediato y material sobre la reputación, las finanzas, las operaciones o la normativa.
    - Los activos con una puntuación de riesgo inherente del 80% o superior se clasifican como críticos.
- **Alto:** Activos de los que Equifax depende en gran medida en el desempeño de un proceso de negocio o componente de dónde podría haber un impacto significativo a través de la pérdida o corrupción de datos de Equifax. Cualquier interrupción, fallo o falta de seguridad

podría tener un impacto significativo en la reputación, las finanzas, las operaciones o la normativa.

- Los activos con una puntuación de riesgo inherente inferior al 80%, pero superior al 61%, se clasifican como altos.

• **Medio:** Activos de los que Equifax depende en un grado limitado en el desempeño de un proceso de negocio o componente de dónde podría haber un impacto moderado a través de la pérdida o corrupción de datos de Equifax. Cualquier interrupción, fallo o falta de seguridad podría tener un impacto moderado sobre la reputación, las finanzas, las operaciones o la normativa.

- Los activos con una puntuación de riesgo inherente inferior al 61%, pero superior al 39%, se clasifican como medios.

• **Bajo:** Activos de los que Equifax depende mínimamente en el desempeño de un proceso de negocio o componente de donde podría haber un impacto mínimo o nulo por la pérdida o corrupción de datos de Equifax.

- Los activos con una puntuación de riesgo inherente inferior al 39% se clasifican como bajos.

Figura 1: Clasificación del riesgo inherente

Riesgo inherente Clasificación	Gama
Crítica	> 80%
Alto	> 61% - 80%
Medio	> 39% - 61%
Bajo	≤ 39%

3.2. Cálculo de la calificación de riesgo inherente (IRR)

Equifax calcula el riesgo inherente considerando el impacto y la probabilidad de las amenazas sin tener en cuenta los controles. Los criterios utilizados para calcular el TIR se basan en los siguientes atributos de los datos:

• Clasificación **de los datos**: La clasificación de datos de mayor sensibilidad de los datos de Equifax a los que accede, transmite, procesa y/o almacena el activo.

- Clase 5: Consumidores protegidos
- Clase 4: Restringido
- Clase 3: Confidencial
- Clase 2: Sólo para uso interno
- Clase 1: Sin restricciones

• **Volumen de datos**: La cantidad total de registros de Equifax a los que se ha accedido, transmitido, procesado y/o almacenado por el activo.

- >100 millones de registros
- >10 millones de registros - <100 millones de registros
- >1 millón de registros - <10 millones de registros
- >100.000 registros - 1 millón de registros
- <100.000 registros

• **Disponibilidad**: La cantidad máxima de tiempo permitida para que un activo no esté disponible antes de impactar en el negocio, representada por el Objetivo de Tiempo de Recuperación (RTO).

- 0 - 1 hora
- > 1 hora - 6 horas
- > 6 horas - 24 horas
- > 24 horas - 72 horas
- < 72 horas

• **Orientación a Internet**: La capacidad de acceder a un activo fuera del entorno de red de Equifax.

Figura 2: Cálculo de la calificación de riesgo inherente

Atributo IRR	Peso
Clasificación de los datos	35% +

Atributo IRR	Peso
Volumen de datos	35%

Atributo IRR	Peso
Disponibilidad	15%

Atributo IRR	Peso
Página web	15%

Calificación del riesgo inherente	Rango
Crítico	> 80%
Alto	> 61% - 80%
Medio	> 39% - 61%
Bajo	≤ 39%

4. Análisis de riesgos

4.1. Clasificación de la evaluación del control (CAR)

El siguiente paso en el ciclo de vida de la evaluación de riesgos es determinar la Calificación de Evaluación de Controles (CAR) utilizando el Cuestionario de Evaluación de Controles (CAQ). La siguiente tabla representa los controles de seguridad clave de Equifax alineados con el Marco de Ciberseguridad del NIST (CSF).

Figura 3: Controles de seguridad clave

Identificador de la función	Identificador de la función	Identificador de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión de riesgos en la cadena de suministro
PR	Proteger	PR.AC	Gestión de la identificación y control de acceso
		PR.AT	Concienciación y formación
		PR.DS	Seguridad de los datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de la seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de la respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación

		RS.IM	Mejoras
RC	Recuperar	RC.RP	Recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

4.2. Cálculo de la calificación de control (CAR)

El CAQ analiza la eficacia operativa de los controles de seguridad dentro del entorno que mitiga el riesgo. El CAR se determina calculando el conjunto de respuestas de control (es decir, Incompleto, Inicial, Gestionado, Definido, Gestionado Cuantitativamente y Optimizado). Las calificaciones de CAR y los rangos numéricos se proporcionan a continuación.

Figura 4: Valoración del control

Controlar Calificación de la evaluación	Gama
Adecuado	≥ 95%
Necesita mejorar	< 95% - 84%
Inadecuado	< 84%

5. Evaluación de riesgos

5.1. Calificación de riesgo residual (RRR)

El riesgo residual es el nivel de riesgo que queda después de tener en cuenta los controles. El RRR se define como sigue:

- **Crítico: Un evento** de amenaza podría resultar en la explotación de debilidades de control y causar efectos adversos severos en las operaciones de la organización. Un evento podría tener un impacto inmediato y material sobre la reputación, las finanzas, las operaciones o la normativa.
- **Alto: Un evento** de amenaza podría resultar en la explotación de debilidades de control y causar efectos adversos significativos en las operaciones de la organización. Un evento podría tener un impacto significativo en la reputación, las finanzas, las operaciones o la normativa.
- **Media: Un evento** de amenaza podría resultar en la explotación de debilidades de control y causar efectos adversos moderados en las operaciones de la organización. Un evento podría tener un impacto moderado sobre la reputación, las finanzas, las operaciones o la normativa.

- **Baja: Un evento** de amenaza podría resultar en la explotación de debilidades de control y causar efectos adversos mínimos en las operaciones de la organización. Un evento podría tener un impacto mínimo en la reputación, las finanzas, las operaciones o la normativa.

5.2. Cálculo de la calificación de riesgo residual

Una vez determinados la IRR y el CAR, se puede calcular la TIR. La fórmula para calcular el riesgo residual es la siguiente:

Riesgo inherente - eficacia del control = Riesgo Residual

A continuación se resumen los resultados de todas las posibles calificaciones de riesgo residual resultantes de la combinación de las calificaciones de riesgo inherente y de evaluación de control:

Figura 5: Calificación de riesgo residual (RRR)

Calificación de riesgo residual (RRR)		Clasificación de la evaluación del control (CAR)		
		Adecuado	Necesita mejorar	Inadecuado
Calificación de riesgo inherente (IRR)	Crítica	Medio	Alto	Crítico
	Alto	Bajo	Medio	Alto
	Medio	Bajo	Bajo	Medio
	Bajo	Bajo	Bajo	Bajo

5.3. Resultados de la evaluación de riesgos

Los resultados de la evaluación de los riesgos de seguridad incluyen el IRR, el CAR y el RRR. Los resultados se comunican al propietario del activo y a las partes interesadas correspondientes.

6. Tratamiento del riesgo

El equipo de riesgos de seguridad global es responsable de informar de los problemas identificados al equipo de gestión de problemas. El progreso de los esfuerzos de remediación se revisa periódicamente y se informa a la alta dirección. Los problemas identificados se clasifican de la siguiente manera:

Figura 6: Clasificación de los problemas de evaluación de los riesgos de seguridad

Cuestiones Calificación del impacto		Prioridad de control			
		Prioridad 3	Prioridad 2	Prioridad 1	Prioridad 0
Calificación del riesgo inherente	Crítica	Medio	Alto	Alto	Crítico
	Alto	Medio	Medio	Alto	Crítico
	Medio	Bajo	Medio	Medio	Alto
	Bajo	Bajo	Bajo	Medio	Medio

Ejemplo: Un activo con una TIR crítica y una prioridad de control 1, da lugar a una calificación de impacto de emisión alta.

El impacto de las deficiencias de control se describe a continuación:

Figura 7: Descripciones de la calificación del impacto de los problemas

Calificación del impacto de la emisión	Emisión Calificación Descripción
Crítico	• Las deficiencias de control podrían dar lugar a una grave exposición al riesgo de la organización. • Las deficiencias requieren la máxima prioridad de remediación, con un seguimiento de los progresos e informes periódicos a la dirección.
Alto	• Las deficiencias de control podrían dar lugar a una importante exposición al riesgo de la organización. • Las deficiencias requieren una alta prioridad de remediación con un progreso monitoreado y reportado a la gerencia periódicamente.
Medio	• Las deficiencias de control podrían dar lugar a una exposición moderada al riesgo organizativo. • Las deficiencias requieren una prioridad de remediación moderada con un seguimiento del progreso.
Bajo	• Las deficiencias de control podrían dar lugar a una exposición mínima al riesgo de la organización. • Las deficiencias deben abordarse a medida que el tiempo y los recursos lo permitan.

7. Control de riesgos

Los resultados de las evaluaciones de riesgos se basan en un punto en el tiempo, por lo que las actividades de reevaluación garantizan que los riesgos se mantengan en un nivel tolerable. La cadencia de reevaluación se basa en la IRR que se indica en el cuadro siguiente:

IRR	Cadencia de reevaluación
Crítico	cada 12 meses
Alta	cada 18 meses
Media	cada 2 años
Baja	cada 3 años

Figura 8: IRR y cadencia de reevaluación asociada