Procedimiento de Gestión de Incidentes de Seguridad

Medical Solutions Colombia SA

1. Objetivos

Establecer las actividades de la gestión de incidentes para Medical Solutions Colombia SA, alineadas a la Política de Seguridad de la Información implementada por la compañía, con el objeto de mantener las plataformas e infraestructura tecnológica y establecer las medidas correctivas y preventivas necesarias.

2. Alcance

Este documento abarca a los incidentes que puedan ocurrir en el ámbito de los activos que dan soporte a los servicios que brinda la compañía; alcanza de la recepción de notificación de la incidencia, su resolución y registro de ocurrencia.

3. Definiciones

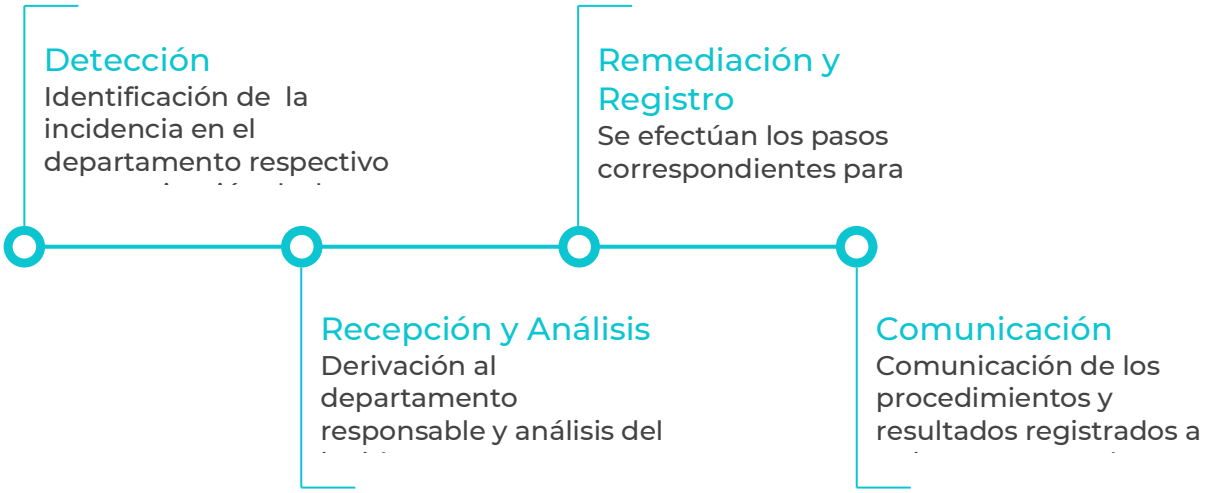
Incidencia: Un único evento o serie de eventos de seguridad de la información inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.
Contingencia: Acción correctiva frente a una incidencia.
Procedimiento: Normas y/o pasos predefinidos para actuar frente a una situación, normalmente establecido mediante políticas internas.
Plan: Hace referencia a este documento en general y lo que afecta.

4. Vigencia

Este plan entrará en vigencia a partir del día XX de XXXX de 202X

5. Sinópsis

A continuación se describen los pasos a seguir, desde la identificación de una incidencia hasta la resolución de la misma:



6. Procedimiento

A continuación se describen los procesos que deberán seguir los funcionarios para la resolución de los incidentes de acuerdo a la fase en la que se encuentren:

Detección

Identificación de un incidente y comunicación de la situación inicial
Ante un suceso de cualquier naturaleza que afecte o ponga en peligro el normal funcionamiento de una actividad de forma segura y que no cuente con una solución directa o protocolizada, se deberá: • Identificar y detallar las circunstancias en las que ocurre el incidente. • Contactar al responsable de la detección de incidentes (Esteban Galindo). • Enviar documentación asociada al incidente. En caso de que la identificación de un incidente se realice mediante un sistema automatizado, se deberá generar una notificación, como por ejemplo un ticket, para su análisis. En caso de que un incidente no se haya detectado inmediatamente, se deberá proceder a detallar la circunstancia de detección y de ser posible el contexto de ocurrencia.

Entradas	
Obligatorias	Detección de un incidente
Opcionales	Registro automático de la ocurrencia de un incidente.

Roles y Responsabilidades	
Responsable	Será responsable quien identifique el incidente o responsable de la plataforma que identifica automáticamente el incidente.
Aprobador	-
Consultado	-
Informado	Esteban Galindo

Salidas	
Obligatorias	Mensaje con los detalles del incidente mediante correo electrónico o ticket. Formulario y documentación de reColombia SAldo.
Opcionales	Mensaje de notificación a través de medio de comunicación alternativo.
Plantillas	Anexo 1: Formulario de Detección de Incidente
Herramientas	Correo electrónico

Recepción y Análisis

Recepción del incidente y análisis de la situación
Ante la notificación de un incidente, mediante email, alertas u otro medio, Esteban Galindo, con ayuda del responsable de tecnología Cristián Farias, determinan el curso a seguir en la resolución del incidente según su clasificación: • Incidentes no intencionales o involuntarios. • Daños físicos. • Incumplimiento o violación de requisitos y regulaciones legales. • Fallos en las configuraciones. • Denegación de servicio. • Acceso no autorizado, espionaje y/o robo de información. • Borrado o pérdida de información. • Infección por código malicioso. • Otro no categorizado. Cada incidente puede derivar a una **medida proactiva para un evento de seguridad** (ej: incorporación de reglas a una Política de Seguridad) o en **medidas reactivas para un incidente de seguridad** (ej: detección de intrusión por malware). Según los diversos parámetros que tenga el área experta del tema, se clasifica. Una vez clasificado el incidente y conocida la gravedad y el tiempo acordado para su resolución, el experto técnico designado debe decidir sobre las medidas necesarias para resolverlo. Adicionalmente, se debe considerar la herramienta de valorización descrita en el "Anexo 5: Material de Apoyo" y considerar si es necesario comunicar a otros involucrados, para lo que se debe analizar respecto a los acuerdos con clientes/socios/proveedores.

Entradas	
Obligatorias	Notificación de incidentes
Opcionales	-

Roles y Responsabilidades	
Responsable	Esteban Galindo
Aprobador	-
Consultado	Cristián Farías

Salidas	
Obligatorias	Derivación al área responsable y pasos a seguir. Formularios y documentación de reColombia SAldo.
Opcionales	-
Plantillas	Anexo 2: Formulario de Registro
Herramientas	Correo electrónico

Informado	Inti Paredes y partes involucradas en caso de ser pertinente		

Remediación y Registro

Implementar remediación basada en el análisi previo y registro de pasos seguidos
El experto técnico designado trata el incidente y una vez que se resuelve, registra toda la información generada durante la detección y tratamiento y, finalmente, se notifica a la persona que envió primero la notificación del incidente que se cerró en caso de que sea pertinente. Toda la información generada durante la detección y tratamiento del incidente es crítica para el tratamiento y/o prevención de posibles incidentes similares en el futuro (base de conocimiento), así como para recopilar evidencia. Las actividades para dar atención a los incidentes pueden ser de varios tipos: **Contención**: Impiden que el incidente afecte otros sistemas, servicios y/o procesos. Se pueden realizar cambios significativos, siempre y cuando se cuente con reColombia SAldos o sitios alternos de trabajo. **Erradicación**: Limpian y remueven la causa del incidente. Se debe identificar la fuente para prevenir una nueva ocurrencia (remover código malicioso, cuentas comprometidas o sitios web). **Recuperación**: Retornan a producción los sistemas, servicios y/o procesos afectados, incluyen acciones como fortalecer las medidas de seguridad, restauración con backups nuevos, reconstrucción de los sistemas desde cero, sustitución de los archivos comprometidos con versiones limpias, instalación de parches, cambio de contraseñas, etcétera. La notificación del incidente corresponde a un mensaje corto indicando el estado de resolución del incidente sin entrar en detalles.

Entradas	
Obligatorias	Notificación del incidente
Opcionales	-
Roles y Responsabilidades	
Responsable	Personal del área capacitado

Salidas	
Obligatorias	Registro de incidentes y resolución. Formularios y documentación de reColombia SAldo.
Opcionales	Recomendaciones para prevención. Notificación a afectados por el incidente.
Plantillas	Anexo 3: Formulario de Remediación

Aprobador	Cristián Farías
Consultado	Moisés Godoy
Informado	- Inti Paredes - Esteban Galindo

Herramientas	-

Comunicación

Comunicación de los sucesos a las partes involucradas e interesadas.

Dependiendo del tipo de incidente identificado y de acuerdo a las reglas de negocio establecidas según las características del cliente (interno o externos), es necesario informar el evento a quien o quienes corresponda.

En estos casos, el responsable técnico emite un informe de incidencia a las partes interesadas en el cual detalla:

- Fecha y hora de aparición del incidente.
- Descripción de la naturaleza de la incidencia.
- Tipología y gravedad del mismo.
- Recursos afectados.
- Posibles orígenes.
- Estado actual del incidente.
- Acciones realizadas para solventarlo y quienes las ejecutaron.
- Fecha y hora de resolución y cierre del incidente.

A diferencia de la notificación, la comunicación del incidente busca detallar lo registrado para el conocimiento de las partes interesadas.

Entradas	
Obligatorias	Registro de incidente
Opcionales	-

Roles y Responsabilidades	
Responsable	Personal del área responsable de la resolución del incidente
Aprobador	Esteban Galindo
Consultado	Cristián Farías
Informado	- Maximiliano Picero - Antonio Lira - Otros interesados

Salidas	
Obligatorias	Informe de Incidencia Formularios y documentación de reColombia SAldo.
Opcionales	-
Plantillas	Anexo 4: Comunicación de Incidencias
Herramientas	Correo electrónico

	pertinentes de acuerdo a la situación.		

7. Anexos

Anexo 1: Formulario de Detección de Incidente

Nombre de quien detecta el incidente	
Fecha de ocurrencia	

Área de detección	**Fecha de Detección**
Descripción	
(Describir el incidente y forma en la que se detecta, en caso de que no se haya detectado con anterioridad indicar fecha de ocurrencia inicial)	
Documentación	**Impacto**
(describir documentación adjunta de reColombia SAldo en caso de que se disponga de ella)	*(Describir brevemente áreas y/o recursos afectados)*

Anexo 2: Formulario de Registro

El formulario a continuación tiene como objetivo mantener registros de los incidentes de seguridad que fueron detectados, y gestionados por Medical Solutions Colombia SA a fin de mantener un análisis retrospectivo de la efectividad de las acciones tomadas.

Detalles Generales

Nombre de Responsable	
Fecha de ocurrencia	
Activos de Información Afectados	
Indique a qué tipo de incidente corresponde Verificar en Procedimiento de Gestión de Incidentes de Seguridad	
Incidente en la Seguridad*	
Evento en la Seguridad de la Información**	
Indique clasificación de origen (Seleccione una o varias opciones)	
Incidentes no intencionales o involuntarios	
Daños físicos	
Incumplimiento o violación de requisitos y regulaciones legales	
Fallos en las configuraciones	
Denegación de servicio	
Acceso no autorizado, espionaje y/o robo de información	

Borrado o pérdida de información	
Infección por código malicioso	
Otro no categorizado	

Indique el Nivel de Urgencia				
1 (Muy Bajo)	2	3	4	5 (Muy Alto)

Indique el Nivel de Impacto				
1 (Muy Bajo)	2	3	4	5 (Muy Alto)

***Incidente de Seguridad: En caso de ser identificado como incidente de seguridad, complete el siguiente apartado.**

Implicancia Seleccione los elementos que se han visto afectados	
Confidencialidad del activo de información	
Integridad del activo de información	
Disponibilidad del activo de información	
Procesos Afectados Explique los principales procesos que vieron afectadas sus operaciones por el Incidente	

El incidente de seguridad ¿Ha identificado una nueva vulnerabilidad sobre el activo?	
Si	No

El incidente de seguridad ¿Ha generado una nueva valorización de los riesgos asociados al activo?		
Si	No	Tal Vez

En caso que las dos respuestas anteriores hayan sido "si", documente y detalle dicho análisis a continuación:

****Evento de Seguridad: En caso de ser identificado como evento de seguridad, complete el siguiente segmento.**

Detalle el potencial de daño en los procesos Identifique procesos afectados y el potencial de daño que implica el evento identificado.

El evento de Seguridad ¿Ha identificado una nueva vulnerabilidad sobre el activo?	
Si	No

El evento de Seguridad ¿Ha generado una nueva valorización de los riesgos asociados al activo?	
Si	No

En caso que las dos respuestas anteriores hayan sido "si", documente y detalle dicho análisis a continuación.

Anexo 3: Formulario de Remediación

Nombre de Responsable	
Fecha de Resolución	
Responsable Indicar el rol del responsable, en caso de ser “Otro” indicarlo.	
Comité de Seguridad de la Información	
Oficial de Seguridad de la Información	
Responsable de Soporte	
Responsable de Tecnología	
Otro	
Detalle de Plan de Resolución	

Anexo 4: Comunicación de Incidencias

Para el registro y comunicación de los incidentes se debe confeccionar un correo que contenga la información esencial (la documentación asociada y formularios anteriores), este deberá ser compartido mediante correo electrónico y/o mediante la plataforma de mensajería interna a las partes interesadas para contar con un reColombia SAldo que valide que fue efectivamente comunicado.

El mensaje debe contar con el siguiente contenido:

Asunto	Reporte de incidencia - [NUM_ID] - [Nombre_Cliente]
Contenido	
Estimados, Les reportamos la siguiente incidencia que hemos identificado:	

Fecha y hora de aparición del incidente: [DD/MM/AAAA - XX:XX hrs]

Descripción de la naturaleza de la incidencia: [descripción]

Tipología y gravedad del mismo: [descripción]

Recursos afectados: [descripción de plataformas, información. Indicar cantidades]

Posibles orígenes: [descripción]

Estado actual del incidente: [pendiente/en resolución/resuelto]

Acciones realizadas para solventarlo y quienes las ejecutaron: [indicar nombre y describir acciones]

Fecha y hora de resolución y cierre del incidente. [DD/MM/AAAA - XX:XX hrs]

Anexo 5: Material de Apoyo

A continuación se presenta un esquema de priorización para clasificación de los incidentes, aquí se describen algunos ejemplos asociados a los niveles de impacto:

Esquema de Priorización		
Nivel	Ejemplo de área de Impacto	Ejemplo de ocurrencia
1 (Muy bajo)	Afectación a la transaccionalidad de un cliente de manera recurrente.	Un cliente recibe un tester en más de una ocasión.
2	Afectación dirigida a un cliente.	Un cliente tiene un incremento de conexiones superior al 50% de su máximo histórico por hora y que parece ser un fraude.
3	Afectación dirigida a un cliente de manera recurrente.	Se repite un patrón de ataque dirigido a un mismo cliente o a cualquier otro en un intervalo de tiempo menor a 15 días.

4	Incidencia de fraude detectada por comercio o por el banco.	Notificación y baja de una afiliación por posible fraude por el banco adquiriente.
5 (Muy alto)	Ataque dirigido con impacto en uno o más clientes.	Ataque DDoS

Dado lo anterior, es importante considerar la siguiente tabla para determinar el nivel de urgencia, destacando en rojo las zonas de alta urgencia y en verde los de baja prioridad, para lo que se considera en un eje el impacto de la incidencia (siguiendo el esquema anterior) mientras que en otro eje indicando la probabilidad de ocurrencia, siendo el nivel 5 un evento Recurrente, el nivel 3 un evento Ocasional y el nivel 1 un evento poco probable:

Tabla de Urgencia						
Probabilidad de Ocurrencia	5	2	3	4	5	5
	4	2	2	3	4	5
	3	1	2	2	3	4
	2	1	1	2	2	3
	1	1	1	1	2	2
	Nivel	1	2	3	4	5
		Impacto / Priorización				

8. Versionado

Confeccionado por	Diego Álvarez
Código de documento	PGI.V1
Versión	V1
Fecha de última actualización	12/05/2021
Revisado por	Esteban Galindo
Aprobado por	