Informe ejecutivo – análisis de riesgos.





SEGURIDAD DE LA

INFORMACIÓN

Análisis de riesgos. Informe ejecutivo.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 1.0 | **Categoría** | Informe |
| **Última actualización** | 30/07/2023 | **Estado** | Aprobado |

# Objetivo

El presente informe contiene un resumen del análisis de riesgos efectuado en el período [fecha desde – fecha hasta]. El documento muestra los riesgos agrupados por nivel según la metodología definida, y el tratamiento para cada grupo.

Este informe debe ser presentado a la Dirección de la organización y sus áreas gerenciales para su consideración y aprobación.

# Alcance

La evaluación de riesgos se realizó sobre [indicar el alcance de la evaluación, por ejemplo, procesos, áreas o sucursales de la organización].

# Metodología

[Los valores utilizados en los criterios son a modo de ejemplo, deben ser establecidos de acuerdo al apetito de riesgo de la organización.]

Para realizar la evaluación de riesgos de acuerdo al alcance establecido, se emplea una metodología de evaluación cualitativa y cuantitativa teniendo en cuenta las siguientes definiciones.

**Escala de impacto.**

|  |  |  |
| --- | --- | --- |
| **Impacto** | **Descripción** | **Valor** |
| Muy Bajo | Puede ocurrir solo en circunstancias excepcionales. | 1 |
| Bajo | Es un suceso raro e infrecuente, aunque no improbable. | 2 |
| Medio | Es posible que ocurra una vez al año | 3 |
| Alto | Es posible que ocurra varias veces en el año | 4 |
| Muy Alto | Es posible que ocurra en periodos menores a 1 año | 5 |

**Escala de probabilidad**

|  |  |  |
| --- | --- | --- |
| Probabilidad | Descripción | Valor |
| Muy Bajo | No se registra adulteración, pérdida, consulta o tratamiento no autorizado, así como desviaciones de información. No hay costos económicos y las operaciones no se ven afectadas. No se registran comentarios adversos que afecten la reputación de la organización. |  1 |
| Bajo | Se registra una consulta o tratamiento no autorizado. Costos económicos extras menores. Las operaciones de negocio no son afectadas significativamente, la interrupción no es percibida por las áreas usuarias. Hay algún comentario adverso externo sin llegar a los medios de comunicación o redes sociales. | 2 |
| Moderado | Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información sin consecuencias significativas. Afecta las operaciones del negocio en hasta un día ocasionando retrabajos que afectan al área de TI. Puede existir un impacto económico importante. Hay comentarios adversos a la organización en los medios o redes sociales. | 3 |
| Alto | Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información con consecuencias significativas. Afecta las operaciones del negocio en más de un día ocasionando retrabajos, la necesidad de contratar servicios adicionales y/o pérdidas económicas. Hay comentarios adversos a la organización en los medios o redes sociales durante más de 1 semana. | 4 |
| Muy Alto | Se registra adulteración, pérdida, consulta o tratamiento no autorizado, o desviaciones de información sensible o confidencial. Afecta las operaciones del negocio, tendiendo a forzar su cierre o reformulación. Tiene un impacto económico significativo. Se daña la reputación de la organización. | 5 |

**Niveles de riesgo.**

[Los colores utilizados en los criterios son a modo de ejemplo, deben ser establecidos de acuerdo al apetito de riesgo de la organización.

En el ejemplo, el apetito está en los valores entre 1 y 4. Entre 5 y 9 tenemos la tolerancia.]

|  |  |
| --- | --- |
|  | Impacto |
| Probabilidad | **1** | **2** | **3** | **4** | **5** |
| **5** | 5 | 10 | 15 | 20 | 25 |
| **4** | 4 | 8 | 12 | 16 | 20 |
| **3** | 3 | 6 | 9 | 12 | 15 |
| **2** | 2 | 4 | 6 | 8 | 10 |
| **1** | 1 | 2 | 3 | 4 | 5 |

Valor entre 1 y 4: Riesgo tolerable.

Valor entre 5 y 9: Riesgo tolerable, pero merece atención.

Valor entre 10 y 25: Riesgo no tolerable, son necesarias acciones.

# Resultado del análisis de riesgos.

Como resultado de la evaluación realizada se descubrieron un total de [n] riesgos con el detalle que se expone a continuación.



Aplicando el criterio de la metodología, se resuelve remediar las 3 vulnerabilidades de severidad alta en el plazo de no más de 30 días, aplicando como control compensatorio [indicar el control compensatorio para evitar riesgo de explotación de la vulnerabilidad].

De las 15 vulnerabilidades de severidad media, [n] resultan en riesgos altos por lo que se decide aplicar controles para mitigarlas.

# Plan de remediación y seguimiento

Las vulnerabilidades de severidad alta (prioridad 1) serán remediadas o mitigadas dentro de los 30 días de halladas. Se aplicarán controles compensatorios dentro de los 7 días de hallada la vulnerabilidad para minimizar el riesgo de explotación.

Las vulnerabilidades de severidad media (prioridad 2) serán remediadas o mitigadas dentro de los 30 días de halladas.

Las vulnerabilidades de severidad baja (prioridad 3) no serán tratadas, si bien se lleva registro de éstas, no se van a tomar acciones. Se cuentan como Aceptadas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Prioridad | Equipo responsable | Fecha de inicio  | Fecha final | Fecha revisión | Responsable revisión |
| 1 | Equipo 1 | dd-mm-aaa | dd-mm-aaaa | dd-mm-aaaa | (cargo) |
| 2 | Equipo 2 | dd-mm-aaaa | dd-mm-aaaa | dd-mm-aaaa | (cargo |

# Recomendaciones

Se recomienda ejecutar un nuevo análisis de vulnerabilidades en el período de 6 meses luego de aplicada la remediación para las 3 vulnerabilidades de severidad alta. Esta recomendación surge de la alta probabilidad de que nuevas vulnerabilidades sean publicadas en ese período.

# Aprobación

Recibido el informe, la dirección de la organización acepta el plan de tratamiento y se compromete a establecer los recursos necesarios para la implementación de las recomendaciones.

|  |  |
| --- | --- |
|  | **Aprobado por** |
| **Fecha de aprobación** | **Cargo** | **Firma** |
|  |  |  |

**Historial de revisiones**

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

