HotelUP

Procedimiento de Identificación de Riesgos

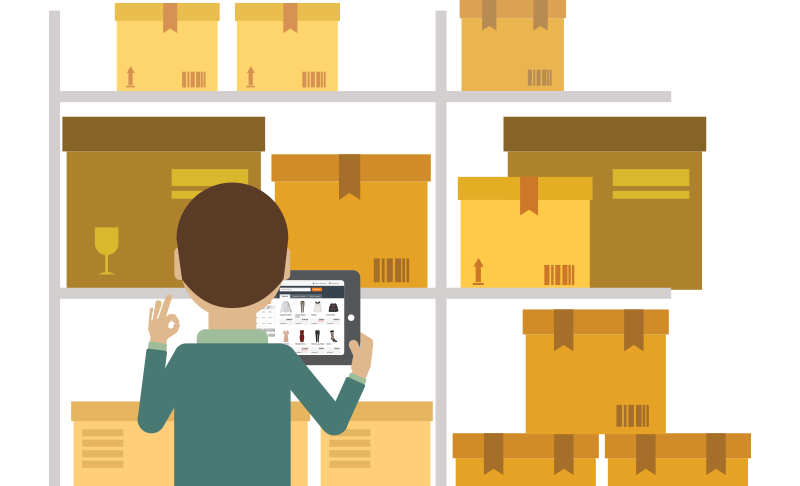
​

1. **DEFINICIONES**
   1. **ACTIVO**

Cualquier recurso de software, hardware, datos o información, datos personales, ubicaciones físicas, personal o comunicaciones relevantes para un proceso.

**Ejemplo:**

Servidores, bases de datos de clientes, red de datos, informacion personal, etc.



* 1. **VULNERABILIDAD**

Debilidad, factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.

**Ejemplo:**

* Cuentas de usuarios sin contraseña.
* No hay software de control de accesos.
* No contar con un plan de recuperación ante desastres.



* 1. **AMENAZA**
* Probabilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria. Una fuente de amenazas no plantea un riesgo cuando no hay vulnerabilidades que pueda ser ‘activadas’.
* Es una circunstancia o evento con la capacidad de cusar daño a un sistema.

**Ejemplo:**

* Terremotos que destruyan el centro de cómputo.



* 1. **IMPACTO**

Es la materialización de un riesgo; una medida del grado de daño o cambio sobre un activo.

**Ejemplo:**

* Retraso en la ejecución y conclusión de actividades de negocio.
* Pérdida de oportunidad y efectividad en la operación.



* 1. **PROBABILIDAD DE OCURRENCIA**
* Posibilidad de que algún hecho se produzca.
* En la terminología de la gestión del riesgo, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algún hecho se produzca, que esta posibilidad está definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o de forma matemática (tales como una probabilidad o una frecuencia sobre un periodo de tiempo dado).



1. **PROCESO DE ANALISIS Y GESTION DEL RIESGO**
   1. **ACTIVIDAD 1: Determinación del Alcance**

Es importante evaluar y entender el contexto de externo e interno de la organización, dado que ambos pueden influir significativamente, en el diseño del marco de trabajo. Por ese motivo se usa el alcance ya determinado en la cláusula 4 de SGSI.

Por ejemplo, considerando los factores internos y externos, las partes interesadas y sus expectativas, se ha definido el alcance del SGSI en 3 procesos:

* 1. **ACTIVIDAD 2: Inventario de Activos**

Para cada proceso mencionado en el alcance se debe realizar un listado de todos los activos que intervienen en cada proceso.

Por ejemplo, en la actividad 1 se definió 3 procesos, entonces se debe realizar 3 listados de activos.

|  |  |  |
| --- | --- | --- |
| Proceso | Descripción | Activos |
| Proceso X | **Comprende …** | **Activo1** |
| **Activo2** |
| **Activo3** |
| **Activo4** |
| **Activo5** |
| **…** |

* 1. **ACTIVIDAD 3: Clasificación de los activos y Asignación de propietarios**

Se debe determinar a qué categoría pertenece cada uno de los activos determinados.

La clasificación de activos no están dentro del ISO 31000 pero se puede complementar, por lo que usamos la metodología MARGERIT, que fue desarrollada por el gobierno español.

|  |  |
| --- | --- |
| **Tipo** | **Clasificación** |
| Resultado de imagen para datos personales png | Datos de carácter personal [DP] |
| Resultado de imagen para base de datos png | Datos/Información [D] |
| Resultado de imagen para foco png | Servicios [S] |
| Resultado de imagen para edificio png | Ubicación Física [U] |
| Resultado de imagen para redes png | Red Comunicaciones [COM] |
| Resultado de imagen para software png | Software [SW] |
| Resultado de imagen para hardware png | Hardware [HW] |
| Resultado de imagen para persona png | Personal [P] |

Cada uno de los activos debe de poseer un propietario. Asimismo, se tiene que especificar quien tiene la asignación de cada uno de los activos.

|  |  |  |  |
| --- | --- | --- | --- |
| **N°** | **DOMINIO** | **ACTIVO** | **PROPIETARIO** |
| **1** | U | Oficina de AAA | GAF |
| **2** | U | Oficina BBB | GCC |
| **3** | U | Oficina CCC | GFS |
| **4** | U | Oficina DDD | GPRC |
| **5** | U | Oficina EEE | GPSU |
| **6** | U | Oficina FFF | GAL |
| **7** | U | Oficina GGG | ST |
| **8** | COM | Red de Datos | GTICE |
| **9** | HW | Central Telefónica | GTICE |
| **10** | HW | Srv AAA | GTICE |
| **11** | SW | SFFF | GTICE |

* 1. **ACTIVIDAD 4: Valoración de Activos**

Se debe determinar los valores de cada uno de los activos en base a su nivel de confidencialidad, disponibilidad e integridad.

1. **Matriz de impacto:**

|  |  |  |
| --- | --- | --- |
| Nivel | Descriptor | Descripción |
| 1 | **Insignificante** | **Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad** |
| 2 | **Menor** | **Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad** |
| 3 | **Dañino** | **Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad** |
| 4 | **Severo** | **Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad** |
| 5 | **Critico** | **Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad** |

1. **Valoración de activos en base al CID:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N°** | **DOMINIO** | **ACTIVO** | **C** | **D** | **I** | **TOTAL** |
| **1** | U | Oficina AAA | 4 | 3 | 2 | 3 |
| **2** | U | Oficina BBB | 4 | 3 | 2 | 3 |
| **3** | U | Oficina CCC | 5 | 5 | 5 | 5 |
| **4** | U | Oficina DDD | 4 | 3 | 1 | 3 |
| **5** | U | Oficina EEE | 4 | 3 | 2 | 3 |
| **6** | U | Oficina FFF | 5 | 5 | 5 | 5 |
| **7** | U | Oficina GGG | 3 | 3 | 2 | 3 |
| **8** | U | Centro de Datos | 5 | 5 | 5 | 5 |
| **9** | COM | Oficina AAA | 5 | 5 | 4 | 5 |
| **10** | HW | Central Telefónica | 4 | 4 | 4 | 4 |
| **11** | HW | SrvAAA | 2 | 5 | 2 | 3 |

* 1. **ACTIVIDAD 5: Detección de Amenazas y Vulnerabilidades**

Luego de tener la lista de activos con sus respectivos propietarios, se debe de analizar bajo que amenaza esta expuesta cada uno de los activos.

Por último, se debe de analizar las vulnerabilidades que pueden aprovechar las amenazas detectadas.

* 1. **ACTIVIDAD 6: Evaluación del Riesgo**

Se debe listar todos los riegos y calcular el dicho riesgo en base a:

* la probabilidad de ocurrencia
* la valoración del impacto.

**CALCULO DEL RIESGO**

Para realizar la evaluación de Riesgo determinaremos 2 variables, la probabilidad de ocurrencia y el impacto que causaría si el riesgo se plasmara, según el ISO 31000 el cálculo del riesgo se determina con estas dos variables:

**RIESGO = PROBABILIDAD DE OCURRENCIA \* VALORACION DEL IMPACTO**

Para ello utilizaremos los siguientes valores:

|  |  |  |
| --- | --- | --- |
| Nivel | Descriptor | Descripción |
| 1 | Insignificante | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad |
| 2 | Menor | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad |
| 3 | Dañino | Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad |
| 4 | Severo | Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad |
| 5 | Critico | Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad |

|  |  |  |  |
| --- | --- | --- | --- |
| Nivel | Descriptor | Descripción | Frecuencia |
| 1 | Raro | El evento ocurre solo en circunstancias excepcionales. | No se ha presentado en los últimos 3 años |
| 2 | Improbable | El evento puede ocurrir en algún momento | Al menos de una vez en los últimos 3 años |
| 3 | Posible | El evento puede ocurrir en algún momento | Al menos de una vez en los últimos 2 años |
| 4 | Probable | El evento probablemente ocurrirá en todas las circunstancias | Al menos de una en el último año |
| 5 | Casi Seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de una vez al año |

* 1. **ACTIVIDAD 7: Aplicación de los Criterios de Aceptación**

Según el resultado del riesgo, se tiene que analizar que cosa hacer con cada uno de los riesgos.

Por ejemplo, para los que están en un nivel extremo o alto, se puede aplicar una contramedida para llevar el riesgo a un nivel aceptable.

Por otro lado, si se tiene un nivel medio o bajo se puede convivir con dichos riesgos. Todo dependerá de los criterios de aceptación de la Alta Dirección de la Empresa.

* 1. **ACTIVIDAD 8: Asignación de los Propietarios del Riesgo**

Una vez ya se tomó una postura para aplicar alguna contramedida en la actividad anterior, se tiene que determinar quién va a implementar dichas salvaguardas y también quien será el dueño de cada uno de sus riegos.

* 1. **ACTIVIDAD 9: Elaboración del Plan de Tratamiento de los Riesgos**

Después de que se calculo el riesgo, se tiene que sugerir un plan que se va a ejecutar.

Por ejemplo, calendario de fechas importantes, los recursos que se utilizarán o los que serán necesarios, etc.

* 1. **ACTIVIDAD 10: Evaluación del Riesgo Residual**

Finalmente, luego de que se implementó alguna contramedida se tiene que medir en qué situación se encuentra el riego y ver cuándo se ha reducido.