|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Nombre | Amenaza | Vulnerabilidad | Suposición | Ocurrencia | Descripción | Responsables / afectados |
| a | Fuga de datos | X | X |  | 80% (.70) | Existe la posibilidad de que exista una fuga de datos de nuestros clientes y proveedores | El responsable sería el encargado de sistemas ya que el acceso al sistema es vulnerable y los afectados seria la empresa |
| b | Soporte inadecuado |  | X |  | 40% (.45) | Aquí hace referencia que puede que no se le dé el seguimiento adecuado a las ordenes porque el sistema no es eficiente | El área de ventas ya que se puede perder ventas por el mal funcionamiento |
| c | Máquinas y herramientas no llegan a tiempo |  |  | X | 20% (.15) | Puede llegar a ocurrir que la persona encargada de ingresar los pedidos de máquinas o herramientas nuevas no las ingrese a tiempo o que el sistema sufra un fallo | El área de producción seria el afectado por lo mismo de que llegan tarde las máquinas, piezas u otras cosas se atrasan las ordenes |
| d | Control de cambios |  | X |  | 65% (.70) | Cuando se necesita cambiar algún programa o actualizarlo y no se le informa al personal puede que se genere un mal uso de este | El responsable es el encargado de sistemas ya que debe de informar de los cambios y explicar si es que existe algún procedimiento diferente |
| f | El software para programar las máquinas y herramientas, no llega a tiempo o no se ha actualizado |  | X |  | 50% (.45) | Si no está el programa o esta desactualizado la producción no será eficiente y atrasara las ordenes ya hechas | El responsable es el del área de sistemas y el afectado principal seria el área de producción |
| g | Inclusión de software malicioso | X |  |  | 85% (.90) | Si por alguna razón un empleado ingresa o instala un software que no sepa de donde proviene o quien es el desarrollador puede hacer que el equipo no funcione de manera correcta | El del área de sistemas |
| h | Ataque de virus | X |  |  | 90% (.90) | Puede que por páginas, programas o dispositivos usb las maquinas tenga virus | El área de sistemas porque debe revisar que el antivirus esté funcionando de manera adecuada |
| i | Falta de firewalls |  |  |  |  |  |  |
| j | Ataques al sitio web | X |  |  | 35% (.45) | El sitio web puede sufrir ataques y si se cae nuestros clientes no tendrán información de acerca de nosotros | El de sistemas debe cuidar que el sitio este arriba siempre y exista un respaldo de la información |
| k | Falta de encriptación a información importante | X |  |  | 85% (.90) | Si la información de valor no está encriptada cualquier persona podría tener acceso a ellos | Todos los que manejen esa información deberían encríptalos para así hacer más seguro el manejo de la misma |
| l | Suficiente seguridad física |  | X |  | 90% (.90) | Se debe cuidar también de manera física quien tiene acceso a la información | El encargado de sistemas |
| m | Fallas en los servicios |  | X |  | 90% (.90) | Que cualquier servicio o recurso físico falle o se descomponga | El área de sistemas le debe dar el mantenimiento adecuado |
| n | Sanciones ambientales |  |  | X | 20% (.15) | Se pueden tener sanciones ambientales por desechar de manera inadecuada materiales electrónicos o residuos peligrosos | El afectado seria la empresa, ya que la multa tendría que ser pagada por la empresa |
| o | Reubicaciones |  |  | X | 20% (.15) | Se debe avisar si existen reubicaciones de máquinas o equipos para hacer más fácil el trabajo |  |
| p | Comunicación entre los distintos departamentos |  | X |  | 80% (.70) | Es importante que todas la reas estén conectada para que los procesos se lleven de manera adecuada y no exista perdida de información | Si no existe la comunicación todas las áreas resultan afectadas |
| q | Pérdida de recursos claves | X |  |  | 90% (.90) | Si se pierden recursos claves, del personal existe la posibilidad de que el trabajo no se realice de manera optima | Todos los empleados y responsables de área deben cuidar y estar pendiente de los recursos y llevar un control de inventarios |
| r | Falta de conocimientos |  | X |  | 80% (.70) | Cuando el personal no está adecuadamente capacitados o no tiene los conocimientos necesarios para manejar algún programa o maquina existe un trabajo deficiente | En lo que respecta con los conocimientos programas y maquina el responsable del área de sistemas debe dar una pequeña capacitación a los empleados para que no hay problemas |
| s | Incumplimientos de controles y licencias | X |  |  | 90% (.90) | En caso de no contar con controles de calidad o licencias se puede perder información y ser acreedores a una multa | El responsable del área de sistemas debe checar que todo esté en orden, porque en caso contrario la empresa será acreedora de una multa |
| t | Existe manual de procedimientos |  | X |  | 40% (.45) | Es importante que exista el manual de procedimientos y que se haga lo que establece para evitar problemas |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Amenaza | Residual | Acumulado | Repercutido | Impacto en Activos | Responsables / afectados |
| a |  |  |  |  |  |  |
| b |  |  |  |  |  |  |
| c |  |  |  |  |  |  |
| d |  |  |  |  |  |  |
| f |  |  |  |  |  |  |
| g |  |  |  |  |  |  |
| h |  |  |  |  |  |  |
| i |  |  |  |  |  |  |
| j |  |  |  |  |  |  |
| k |  |  |  |  |  |  |
| l |  |  |  |  |  |  |
| m |  |  |  |  |  |  |
| n |  |  |  |  |  |  |
| o |  |  |  |  |  |  |
| p |  |  |  |  |  |  |
| q |  |  |  |  |  |  |
| r |  |  |  |  |  |  |
| s |  |  |  |  |  |  |
| t |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Activo | FE | TOA | EPS | EPA |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

\*Ataques de virus h

\*Falta de Firewalls i

\*Ataques sitios web j

\*Falta de encriptación a datos importantes k

\*Suficiente seguridad fìsica l

\*Fallas en los servicios m

\*Sanciones ambientales n

\*Reubicaciones o

\*Comunicaciòn entre los distintos departamentos p

\*Pérdida de recursos clave q

\*Falta de conocimientos r

\*Inclumplimiento con controles y licencias s

\*Existe manual de procedimientos t