# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 1:

# Inventario de activos de información

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

- **Activos del subproceso de Planificación:**

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Interfaz que permite modificar, crear o eliminar algún recurso en el maestro de recursos. La información implicada es la relación de materias primas que usa la empresa para crear sus productos. |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Planificación de Producción** | SIS - 02 | Interfaz para administrar pedidos de materiales | Interfaz que permite administrar el pedido de nuevas materias primas que se necesitan para la manufactura de algún producto determinado. La información implicada es la receta del producto, la relación de materias primas, y los programas de producción (Schedules) |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Resource Processor |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Documentos son las listas de pedidos de materiales. |
| **Planificación de Producción** | SIS - 03 | Interfaz de mantenimiento de productos | Interfaz que permite modificar, crear o eliminar algún producto en el maestro de productos. La información implicada es el portafolio de productos que fabrica la empresa y sus características. |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Planificación de Producción** | DOC - 02 | Documento físico con reportes del maestro de productos. | Documentos impresos que con diversos reportes que se sacan del maestro de productos |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | Interfaz que permite crear nuevas órdenes de producción, es decir programa la cantidad de materiales, cantidad de producción, líneas, hornos, etc. La información que está implicada son las programaciones de producción. |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Planning |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Planificación de Producción** | DOC - 03 | Documento físico con reportes de las órdenes de producción. | Documentos impresos que contienen diversos reportes de las ordenes de producción. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | Interfaz que permite crear y modificar las ordenes de ejecución de producción, que indica la cantidad de operadores, programación de hornos, tiempos de cocción, etc. La información que está implicada es la relacionada a las ordenes de trabajo de producción |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Quick Scheduler |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Planificación de Producción** | DOC - 04 | Documento físico con reportes de las órdenes de producción. | Documentos impresos que contienen diversos reportes de la ejecución de ordenes de producción. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | SIS - 06 | Sistema de seguimiento de producción | Sistema que se usa en todas las fases del proceso de producción para hacer el seguimiento de los materiales, ordenes de proceso, programación de manufactura, gestión de productos terminados, etc. |
| | | | # usuarios= 20 |
| | | | Aplicación: Q-Plant |
| | | | Servidor de 2GB |
| | | | Procesador: Intel Xeon 3.0 GHz |
| | | | Sistema operativo: Windows 2003 Server |
| | | | Motor de base de datos: SQL Server 2008 |
| **Planificación de Producción** | HW - 01 | PC's en el área de Planificación | Procesador: Core i5 |
| | | | Sistema Operativo: Windows XP |
| | | | Discos Duro: 500 GB |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | HW- 02 | Cintas de back up | Cintas de 20 GB para guardar los back up de toda la información sobre panificación almacenada en la plataforma AS400 |
| | | | Proveedor para custodia: Iron Mountain Perú |
| **Planificación de Producción** | HW - 03 | Dispositivo (robot) para generar back ups | Robot que recibe las cintas, y luego copia la información de proceso de planificación en ellas, ejecutando comandos desde la plataforma AS400 |
| **Planificación de Producción** | HW - 04 | Pantalla táctil con aplicación Q-Plant | Pantalla táctil a colores ubicada al inicio de la línea de producción para monitorear la orden de proceso y orden de trabajo que se va a realizar |
| | | | # usuarios= 20 |
| | | | tamaño: 15 pulgadas |
| **Planificación de Producción** | AF - 01 | Cámaras de seguridad | Cámaras de vigilancia ubicadas en las oficinas de planificación. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Planificación de Producción** | AF - 02 | Impresoras | Impresoras ubicadas en las oficinas de planificación. |
| **Planificación de Producción** | SW - 01 | Correo electronico | Correos electrónicos de los usuarios y empleados que participan en este subproceso. |
| | | | Microsoft Exchange Server |
| | | | Microsoft Outlook 2010 |
| **Planificación de Producción** | SW - 02 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Medios de almacenamiento con información confidencial que se encuentran en las oficinas de planeamiento. |

- **Activos del subproceso de Manufactura:**

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | SIS - 07 | Interfaz de trazabilidad de materiales en Producción | Interfaz que permite hacer el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción. |
| | | | # usuarios= 25 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Manufactura** | DOC - 05 | Documento físico con reportes de la trazabilidad de materiales en un programa de producción | Documentos impresos que contienen diversos reportes de la trazabilidad de las transacciones internas de los materiales. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | SIS - 08 | Interfaz de declaración de consumo de materiales | Interfaz que permite al usuario registrar cada consumo de materia prima o material intermedio que se da durante todo el proceso de manufactura. |
| | | | # usuarios= 123 |
| | | | Aplicación: PRISM 7.0i Production Analysis |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Manufactura** | DOC - 06 | Documento físico con reportes de los consumos de materiales | Documentos impresos que contienen diversos reportes de los consumos que se hacen de todos los materiales durante la manufactura. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | SIS - 09 | Interfaz de declaración de producto terminado | Interfaz que permite registrar cada vez que se haya terminado con la manufactura de algunos lotes de productos, es decir cuando se cumpla toda una orden de de producción |
| | | | # usuarios= 123 |
| | | | Aplicación: PRISM 7.0i Production Analysis |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Manufactura** | SIS - 10 | Interfaz de ejecución de Orden de Proceso | Interfaz que permite iniciar la ejecución del la orden de proceso de manufactura. |
| | | | # usuarios= 123 |
| | | | Aplicación: PRISM 7.0i Production Analysis |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | SIS - 11 | Interfaz de Surtimiento de materiales a producción | Interfaz que permite surtir a la manufactura la cantidad necesaria de cada materia prima para la fabricación de determinado producto |
| | | | # usuarios= 25 |
| | | | Aplicación: PRISM 7.0i Quick Scheduler |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Manufactura** | SIS - 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | Interfaz que permite modifica las unidades de medida de cada materia prima, así como las unidades de las cantidades de producción |
| | | | # usuarios= 25 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | SIS - 13 | Sistema de seguimiento de producción | Sistema que se usa en todas las fases del proceso de producción para hacer el seguimiento de los materiales, ordenes de proceso, programación de manufactura, gestión de productos terminados, etc. |
| | | | # usuarios= 123 |
| | | | Aplicación: Q-Plant |
| | | | Servidor de 2GB |
| | | | Procesador: Intel Xeon 3.0 GHz |
| | | | Sistema operativo: Windows 2003 Server |
| | | | Motor de base de datos: SQL Server 2008 |
| **Proceso de Manufactura** | HW - 05 | PC's en planta | Procesador: Core i5 |
| | | | Sistema Operativo: Windows XP |
| | | | Discos Duro: 500 GB |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | HW - 06 | Cintas de back up | Cintas de 20 GB para guardar los back up de toda la información del proceso de manufactura almacenada en la plataforma AS400 |
| | | | Proveedor para custodia: Iron Mountain Perú |
| **Proceso de Manufactura** | HW - 07 | Dispositivo (robot) para generar back ups | Robot que recibe las cintas, y luego copia la información del proceso de manufactura en ellas, ejecutando comandos desde la plataforma AS400 |
| **Proceso de Manufactura** | HW - 08 | Pantallas táctiles con aplicación Q-Plant | Pantallas táctiles a colores ubicadas a lo largo de la línea de producción para monitorear todo el proceso de manufactura |
| | | | # Usuarios = 20 |
| | | | tamaño: 15 pulgadas |
| **Proceso de Manufactura** | AF - 03 | Cámaras de seguridad | Cámaras de vigilancia ubicadas en las áreas de manufactura. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Manufactura** | AF - 04 | Impresoras | Impresoras ubicadas en las áreas de manufactura. |
| **Proceso de Manufactura** | SW - 03 | Correo electronico | Correos electrónicos de los usuarios y empleados que participan en este subproceso. |
| | | | Microsoft Exchange Server |
| | | | Microsoft Outlook 2010 |
| **Proceso de Manufactura** | SW - 04 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Medios de almacenamiento que se encuentran en las áreas de manufactura. |

- **Activos del subproceso de Calidad:**

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Interfaz que permite realizar el mantenimiento de los controles de calidad de los productos. |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Quality Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Calidad** | DOC - 07 | Documento físico con reportes de resultados de los controles de calidad | Documentos impresos que contienen diversos reportes de resultados obtenidos en las pruebas de calidad de los productos. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Calidad** | SIS - 15 | Interfaz de gestión de calidad | Interfaz que permite gestionar los niveles de calidad que tendrán los productos. |
| | | | # usuarios= 20 |
| | | | Aplicación: PRISM 7.0i Quality Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Proceso de Calidad** | DOC - 08 | Documento físico con los niveles de calidad que tendrán los productos. | Documentos impresos que contienen los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Calidad** | SIS - 16 | Sistema de seguimiento de producción (q-plant) | Sistema que se usa en todas las fases del proceso de producción para hacer el seguimiento de los materiales, ordeneces de proceso, programación de manufactura, gestión de productos terminados, etc. |
| | | | # usuarios= 20 |
| | | | Aplicación: Q-Plant |
| | | | Servidor de 2GB |
| | | | Procesador: Intel Xeon 3.0 GHz |
| | | | Sistema operativo: Windows 2003 Server |
| | | | Motor de base de datos: SQL Server 2008 |
| **Proceso de Calidad** | HW - 09 | PC's en las oficinas de Calidad | Procesador: Core i5 |
| | | | Sistema Operativo: Windows XP |
| | | | Discos Duro: 500 GB |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Proceso de Calidad** | HW - 10 | Cintas de back up | Cintas de 20 GB para guardar los back up de toda la información del proceso de calidad almacenada en la plataforma AS400 |
| | | | Proveedor para custodia: Iron Mountain Perú |
| **Proceso de Calidad** | HW - 11 | Dispositivo (robot) para generar back ups | Robot que recibe las cintas, y luego copia la información del proceso de calidad en ellas, ejecutando comandos desde la plataforma AS400 |
| **Proceso de Calidad** | HW - 12 | Pantallas táctiles con aplicación Q-Plant | Pantallas táctiles a colores ubicadas a lo largo de la línea de producción para monitorear todo el proceso de manufactura |
| | | | # Usuarios = 20 |
| | | | tamaño: 15 pulgadas |
| **Proceso de Calidad** | AF - 05 | Cámaras de seguridad | Cámaras de vigilancia ubicadas en las oficinas de calidad. |

| | | | |
|---|---|---|---|
| **Proceso de Calidad** | AF - 06 | Impresoras | Impresoras ubicadas en las áreas de calidad. |
| **Proceso de Calidad** | SW - 05 | Correo electronico | Correos electrónicos de los usuarios y empleados que participan en este subproceso. |
| | | | Microsoft Exchange Server |
| | | | Microsoft Outlook 2010 |
| **Proceso de Calidad** | SW - 06 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Medios de almacenamiento que se encuentran en las oficinas de calidad. |

- **Activos del subproceso de Calidad:**

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | SIS - 17 | Interfaz de generación de reportes de inventarios | Interfaz que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa en cierto momento. |
| | | | # usuarios= 17 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Bodegas e inventarios** | DOC - 09 | Documento físico con los reportes de inventarios | Documentos impresos que contienen los distintos reportes de inventarios de las bodegas y almacenes de la empresa. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | SIS - 18 | Interfaz de entrega de salida de productos terminados | Interfaz que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes o puntos de distribución. |
| | | | # usuarios= 17 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |
| **Bodegas e inventarios** | SIS - 19 | Interfaz para traslado de materias primas y productos entre plantas | Interfaz que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa |
| | | | # usuarios= 17 |
| | | | Aplicación: PRISM 7.0i Resource Management |
| | | | Plataforma: AS400 |
| | | | Tipo de aplicación: Cliente/Servidor (Package) |
| | | | Servidor de base de datos relacional: IBM DB2 |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | SIS - 20 | Sistema de seguimiento de producción (q-plant) | Sistema que se usa en todas las fases del proceso de producción para hacer el seguimiento de los materiales, ordeneces de proceso, programación de manufactura, gestión de productos terminados, etc. |
| | | | |
| | | | # usuarios= 20 |
| | | | Aplicación: Q-Plant |
| | | | Servidor de 2GB |
| | | | Procesador: Intel Xeon 3.0 GHz |
| | | | Sistema operativo: Windows 2003 Server |
| | | | Motor de base de datos: SQL Server 2008 |
| **Bodegas e inventarios** | DOC - 10 | Kardex de mercancía en almacén | Registro en Microsoft Excel de la mercancía almacenada en las bodegas. Este registro contiene toda la información de las mercancías como cantidad, valor de medida, precio, etc. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | HW - 13 | PC's en las bodegas y almacenes | Procesador: Core i5 |
| | | | Sistema Operativo: Windows XP |
| | | | Discos Duro: 500 GB |
| **Bodegas e inventarios** | HW - 14 | Cintas de back up | Cintas de 20 GB para guardar los back up de toda la información de bodegas e inventarios almacenada en la plataforma AS400 |
| | | | Proveedor para custodia: Iron Mountain Perú |
| **Bodegas e inventarios** | HW - 15 | Dispositivo (robot) para generar back ups | Robot que recibe las cintas, y luego copia la información de las bodegas e inventarios en ellas, ejecutando comandos desde la plataforma AS400 |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | HW - 16 | Pantallas táctiles con aplicación Q-Plant | Pantalla táctil a colores ubicada al final de la línea de producción para monitorear el almacenaje de los productos terminados. |
| | | | tamaño: 15 pulgadas |
| **Bodegas e inventarios** | AF - 07 | Cámaras de seguridad | Camaras de vigilancia ubicadas en las bodegas y almacenes. |
| **Bodegas e inventarios** | AF - 08 | Impresoras | Impresoras ubicadas en las bodegas y almacenes. |

| Subproceso | Id | Activo | Características |
|---|---|---|---|
| **Bodegas e inventarios** | SW - 07 | Correo electronico | Correos electrónicos de los usuarios y empleados que participan en este subproceso. |
| | | | Microsoft Exchange Server |
| | | | Microsoft Outlook 2010 |
| **Bodegas e inventarios** | SW - 08 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Medios de almacenamiento que se encuentran en las bodegas o almadenes. |

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 2: Vulnerabilidades y amenazas de los activos de información

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

- **Vulnerabilidades y amenazas de los activos del subproceso de Planificación:**

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Controles de acceso al sistema inadecuados. | Filtraciones de información y accesos no autorizados el sistema. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Puntos de acceso al sistema remotos a la red privada de la empresa | Accesos de personas no autorizadas al sistema e intercepción de la red |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Sistema operativo vulnerable | Acceso de personas ajenas a la empresa que pueden robar información. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Contraseñas de los usuarios sencillas | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 03 | Interfaz de mantenimiento de productos | Contraseñas de los usuarios sencillas | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Exceso de privilegios para usuarios no indicados | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | Exceso de privilegios para usuarios no indicados | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. |
| | SIS - 06 | Sistema de seguimiento de producción | | |
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Aplicación desactualizada o parchada incorrectamente | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Falta de políticas para el adecuado uso de este sistema | Uso inadecuado de la aplicación y su información por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |
| | SIS - 03 | Interfaz de mantenimiento de productos | | |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |
| **Planificación de Producción** | SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Falta de bitácoras de acceso al sistema | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. |
| | SIS - 02 | Interfaz para administrar pedidos de materiales | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | SIS - 03 | Interfaz de mantenimiento de productos | Falta de bitácoras de acceso al sistema | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. |
| | SIS - 04 | Interfaz de mantenimiento de Ordenes de Producción | | |
| | SIS - 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | | |
| | SIS - 06 | Sistema de seguimiento de producción | | |
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Poca higiene en el lugar donde se guarda el documento. | Deterioro permanente de los documentos. |
| | DOC - 02 | Documento físico con reportes del maestro de productos. | | |
| | DOC - 03 | Documentos impresos que contienen diversos reportes de las órdenes de producción. | | |
| | DOC - 04 | Documento físico con reportes de las órdenes de producción. | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Falta de control de acceso al lugar donde se guarda el documento. | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC - 02 | Documento físico con reportes del maestro de productos. | | |
| | DOC - 03 | Documentos impresos que contienen diversos reportes de las ordenes de producción. | | |
| | DOC - 04 | Documento físico con reportes de las ordenes de producción. | | |
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Falta de manejo adecuado de las copias de los documentos | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC - 02 | Documento físico con reportes del maestro de productos. | | |
| | DOC - 03 | Documentos impresos que contienen diversos reportes de las órdenes de producción. | | |
| | DOC - 04 | Documento físico con reportes de las órdenes de producción. | | |
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Falta de contraseñas y controles para el manejo de las impresoras y fotocopiadoras. | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | DOC - 02 | Documento físico con reportes del maestro de productos. | Falta de contraseñas y controles para el manejo de las impresoras y fotocopiadoras. | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. |
| | DOC - 03 | Documentos impresos que contienen diversos reportes de las ordenes de producción. | | |
| | DOC - 04 | Documento físico con reportes de las ordenes de producción. | | |
| **Planificación de Producción** | DOC - 01 | Documento físico con lista de pedido de materiales | Falta de políticas para el adecuado manejo de documentos impresos, con información importante. | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. |
| | DOC - 02 | Documento físico con reportes del maestro de productos. | | |
| | DOC - 03 | Documentos impresos que contienen diversos reportes de las órdenes de producción. | | |
| | DOC - 04 | Documento físico con reportes de las órdenes de producción. | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | HW - 01 | PC's en el área de Planificación | Falta de control de acceso al lugar donde se encuentra las PC's | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. |
| | | | Falta de bitácoras de acceso a la PC. | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de Planificación por parte de cada usuario. |
| | | | Falta de correcta identificación de usuarios y contraseñas para acceder a la PC. | Filtraciones de información y accesos no autorizados a las PC's de la oficina de planificación por parte de usuarios no autorizados o ajenos a la empresa. |
| | | | Falta de seguridad de la red interna median la cual están interconectadas las PC's | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización. |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Planificación de Producción** | HW - 02 | Cintas de back up | Falta de control de acceso al lugar donde se encuentra guardadas las cintas. | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Poca higiene en el lugar donde se guarda las cintas. | Deterioro permanente de las cintas. |
| **Planificación de Producción** | HW - 03 | Dispositivo (robot) para generar back ups | Falta de control de acceso al lugar donde se encuentra el robot. | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Falta de control para el manejo del robot. | Manejo del robot por parte de personas ajenas a la empresa o sin autorización |
| **Planificación de Producción\|** | HW - 04 | Pantalla táctil con aplicación Q-Plant | Falta de correcta identificación de usuarios y contraseñas para acceder a la pantalla. | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Ubicación inadecuada de la pantalla. | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación |
| **Planificación de Producción\|** | AF - 01 | Cámaras de seguridad | Falta de control de acceso a la central de vigilancia donde se encuentra los monitores y demás equipos donde se ven las imágenes de las cámaras. | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. |
| | | | Ubicación inadecuada de las cámaras. | Facilidad de manipulación de las cámaras por parte de personal no autorizado. |

| | | | | |
|---|---|---|---|---|
| **Planificación de Producción** | AF - 02 | Impresoras | Falta de contraseñas y controles para el manejo de las impresoras. | Facilidad de acceso y manejo de la impresora del área de planificación por parte de personas sin autorización y ajenas al subproceso o a la empresa. |
| | | | Falta de bitácoras de seguimiento del manejo de la impresora. | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de Planificación por parte de cada usuario. |
| **Planificación de Producción** | SW - 01 | Correo electrónico | Falta de Antivirus y Antispam para contrarrestar los virus que puedan contener los correos maliciosos. | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. |
| | | | Mala configuración de los firewall | Accesos maliciosos mediante correos electrónicos. |
| | | | Falta de protección de los servidores de correo electronico | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. |
| | | | Acceso remoto al correo electronico poco seguro | Acceso al correo electronico de los usuarios del área de planificación por parte de personas no autorizadas. |
| | | | Falta de políticas para el correcto uso del correo electronico de la empresa. | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. |
| **Planificación de Producción** | SW - 02 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Falta de control de acceso al lugar donde se encuentra guardados los medios de almacenamiento. | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. |

- **Vulnerabilidades y amenazas de los activos del subproceso de Manufactura:**

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Controles de acceso al sistema inadecuados. | Filtraciones de información y accesos no autorizados el sistema. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Puntos de acceso al sistema remotos a la red privada de la empresa | Accesos de personas no autorizadas al sistema e intercepción de la red |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **ceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Sistema operativo vulnerable | Acceso de personas ajenas a la empresa que pueden robar información. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Contraseñas de los usuarios sencillas | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Exceso de privilegios para usuarios no indicados | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Aplicación desactualizada o parchada incorrectamente | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Falta de políticas para el adecuado uso de este sistema | Uso inadecuado de la aplicación y su información por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SIS – 07 | Interfaz de trazabilidad de materiales en Producción | Falta de bitácoras de acceso al sistema | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. |
| | SIS – 08 | Interfaz de declaración de consumo de materiales | | |
| | SIS – 09 | Interfaz de declaración de producto terminado | | |
| | SIS – 10 | Interfaz de ejecución de Orden de Proceso | | |
| | SIS – 11 | Interfaz de Surtimiento de materiales a producción | | |
| | SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | | |
| | SIS – 13 | Sistema de seguimiento de producción | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | DOC – 05 | Documento físico con lista de pedido de materiales | Poca higiene en el lugar donde se guarda el documento. | Deterioro permanente de los documentos. |
| | DOC – 06 | Documento físico con reportes del maestro de productos. | | |
| **Proceso de Manufactura** | DOC – 05 | Documento físico con lista de pedido de materiales | Falta de control de acceso al lugar donde se guarda el documento. | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC – 06 | Documento físico con reportes del maestro de productos. | | |
| **Proceso de Manufactura** | DOC – 05 | Documento físico con lista de pedido de materiales | Falta de manejo adecuado de las copias de los documentos | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC - 06 | Documento físico con reportes del maestro de productos. | | |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | DOC – 05 | Documento físico con lista de pedido de materiales | Falta de contraseñas y controles para el manejo de las impresoras y fotocopiadoras. | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados |
| | DOC – 06 | Documento físico con reportes del maestro de productos. | | |
| **Proceso de Manufactura** | DOC – 05 | Documento físico con lista de pedido de materiales | Falta de políticas para el adecuado manejo de documentos impresos, con información importante. | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. |
| | DOC – 06 | Documento físico con reportes del maestro de productos. | | |
| **Proceso de Manufactura** | HW - 05 | PC's en planta | Falta de control de acceso al lugar donde se encuentra las PC's | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. |
| | | | Falta de bitácoras de acceso a la PC. | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de Planificación por parte de cada usuario. |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | HW - 05 | PC's en planta | Falta de correcta identificación de usuarios y contraseñas para acceder a la PC. | Filtraciones de información y accesos no autorizados a las PC's de la oficina de planificación por parte de usuarios no autorizados o ajenos a la empresa. |
| | | | Falta de seguridad de la red interna median la cual están interconectadas las PC's | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización. |
| **Proceso de Manufactura** | HW – 06 | Cintas de back up | Falta de control de acceso al lugar donde se encuentra guardadas las cintas. | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Poca higiene en el lugar donde se guarda las cintas. | Deterioro permanente de las cintas. |
| **Proceso de Manufactura** | HW – 07 | Dispositivo (robot) para generar back ups | Falta de control de acceso al lugar donde se encuentra el robot. | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Falta de control para el manejo del robot. | Manejo del robot por parte de personas ajenas a la empresa o sin autorización |
| **Proceso de Manufactura** | HW - 08 | Pantalla táctil con aplicación Q-Plant | Falta de correcta identificación de usuarios y contraseñas para acceder a la pantalla. | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Ubicación inadecuada de la pantalla. | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | AF - 03 | Cámaras de seguridad | Falta de control de acceso a la central de vigilancia donde se encuentra los monitores y demás equipos donde se ven las imágenes de las cámaras. | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. |
| | | | Ubicación inadecuada de las cámaras. | Facilidad de manipulación de las cámaras por parte de personal no autorizado. |
| **Proceso de Manufactura** | AF - 04 | Impresoras | Falta de contraseñas y controles para el manejo de las impresoras. | Facilidad de acceso y manejo de la impresora del área de planificación por parte de personas sin autorización y ajenas al subproceso o a la empresa. |
| | | | Falta de bitácoras de seguimiento del manejo de la impresora. | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de Planificación por parte de cada usuario. |
| **Proceso de Manufactura** | SW - 03 | Correo electrónico | Falta de Antivirus y Antispam para contrarrestar los virus que puedan contener los correos maliciosos. | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. |
| | | | Mala configuración de los firewall | Accesos maliciosos mediante correos electrónicos. |
| | | | Falta de protección de los servidores de correo electronico | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. |
| | | | Acceso remoto al correo electronico poco seguro | Acceso al correo electronico de los usuarios del área de planificación por parte de personas no autorizadas. |
| | | | Falta de políticas para el correcto uso del correo electronico de la empresa. | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. |

| Subproceso | Id | Activo | Vulnerabilidad | Amenaza |
|---|---|---|---|---|
| **Proceso de Manufactura** | SW - 04 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Falta de control de acceso al lugar donde se encuentra guardados los medios de almacenamiento. | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. |

- **Vulnerabilidades y amenazas de los activos del subproceso de Calidad:**

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Controles de acceso al sistema inadecuados. | Filtraciones de información y accesos no autorizados el sistema. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Puntos de acceso al sistema remotos a la red privada de la empresa | Accesos de personas no autorizadas al sistema e intercepción de la red |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Sistema operativo vulnerable | Acceso de personas ajenas a la empresa que pueden robar información. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Exceso de privilegios para usuarios no indicados | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Aplicación desactualizada o parchada incorrectamente. | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Falta de políticas para el adecuado uso de este sistema | Uso inadecuado de la aplicación por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | SIS - 14 | Interfaz de control del procesos de Calidad | Falta de bitácoras de acceso al sistema | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. |
| | SIS - 15 | Interfaz de gestión de calidad | | |
| | SIS - 16 | Sistema de seguimiento de producción (q-plant) | | |
| **Proceso de Calidad** | DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Poca higiene en el lugar donde se guarda el documento. | Deterioro permanente de los documentos. |
| | DOC – 08 | Documento físico con los niveles de calidad que tendrán los productos. | | |
| **Proceso de Calidad** | DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Falta de control de acceso al lugar donde se guarda el documento. | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC – 08 | Documento físico con los niveles de calidad que tendrán los productos. | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Falta de manejo adecuado de las copias de los documentos | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | DOC - 08 | Documento físico con los niveles de calidad que tendrán los productos. | | |
| **Proceso de Calidad** | DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Falta de contraseñas y controles para el manejo de las impresoras y fotocopiadoras. | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados |
| | DOC – 08 | Documento físico con los niveles de calidad que tendrán los productos. | | |
| **Proceso de Calidad** | DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Falta de políticas para el adecuado manejo de documentos impresos, con información importante. | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. |
| | DOC – 08 | Documento físico con los niveles de calidad que tendrán los productos. | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | HW - 09 | PC's en las oficinas de Calidad | Falta de control de acceso al lugar donde se encuentra las PC's | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. |
| | | | Falta de bitácoras de acceso a la PC. | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de Planificación por parte de cada usuario. |
| | | | Falta de correcta identificación de usuarios y contraseñas para acceder a la PC. | Filtraciones de información y accesos no autorizados a las PC's de la oficina de planificación por parte de usuarios no autorizados o ajenos a la empresa. |
| | | | Falta de seguridad de la red interna median la cual están interconectadas las PC's | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización. |
| **Proceso de Calidad** | HW – 10 | Cintas de back up | Falta de control de acceso al lugar donde se encuentra guardadas las cintas. | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Poca higiene en el lugar donde se guarda las cintas. | Deterioro permanente de las cintas. |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | HW – 11 | Dispositivo (robot) para generar back ups | Falta de control de acceso al lugar donde se encuentra el robot. | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Falta de control para el manejo del robot. | Manejo del robot por parte de personas ajenas a la empresa o sin autorización |
| **Proceso de Calidad** | HW - 12 | Pantalla táctil con aplicación Q-Plant | Falta de correcta identificación de usuarios y contraseñas para acceder a la pantalla. | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Ubicación inadecuada de la pantalla. | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación |
| **Proceso de Calidad** | AF - 05 | Cámaras de seguridad | Falta de control de acceso a la central de vigilancia donde se encuentra los monitores y demás equipos donde se ven las imágenes de las cámaras. | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. |
| | | | Ubicación inadecuada de las cámaras. | Facilidad de manipulación de las cámaras por parte de personal no autorizado. |
| **Proceso de Calidad** | AF - 06 | Impresoras | Falta de contraseñas y controles para el manejo de las impresoras. | Facilidad de acceso y manejo de la impresora del área de planificación por parte de personas sin autorización y ajenas al subproceso o a la empresa. |
| | | | Falta de bitácoras de seguimiento del manejo de la impresora. | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de Planificación por parte de cada usuario. |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Proceso de Calidad** | SW – 05 | Correo electrónico | Falta de Antivirus y Antispam para contrarrestar los virus que puedan contener los correos maliciosos. | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. |
| | | | Mala configuración de los firewall | Accesos maliciosos mediante correos electrónicos. |
| | | | Falta de protección de los servidores de correo electronico | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. |
| | | | Acceso remoto al correo electronico poco seguro | Acceso al correo electronico de los usuarios del área de planificación por parte de personas no autorizadas. |
| | | | Falta de políticas para el correcto uso del correo electronico de la empresa. | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. |
| **Proceso de Calidad** | SW - 06 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Falta de control de acceso al lugar donde se encuentra guardados los medios de almacenamiento. | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. |

- **Vulnerabilidades y amenazas de los activos del subproceso de Bodegas e inventarios:**

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Controles de acceso al sistema inadecuados. | Filtraciones de información y accesos no autorizados el sistema. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS - 20 | Sistema de seguimiento de producción (q-plant) | | |
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Puntos de acceso al sistema remotos a la red privada de la empresa. | Accesos de personas no autorizadas al sistema e intercepción de la red. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS - 20 | Sistema de seguimiento de producción (q-plant) | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Sistema operativo vulnerable | Acceso de personas ajenas a la empresa que pueden robar información. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS – 20 | Sistema de seguimiento de producción (q-plant) | | |
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Exceso de privilegios para usuarios no indicados | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS - 20 | Sistema de seguimiento de producción (q-plant) | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Aplicación desactualizada o parchada incorrectamente. | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS – 20 | Sistema de seguimiento de producción (q-plant) | | |
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Falta de políticas para el adecuado uso de este sistema | Uso inadecuado de la aplicación por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS - 20 | Sistema de seguimiento de producción (q-plant) | | |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | SIS – 17 | Interfaz de generación de reportes de inventarios | Falta de bitácoras de acceso al sistema | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. |
| | SIS – 18 | Interfaz de entrega de salida de productos terminados | | |
| | SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | | |
| | SIS – 20 | Sistema de seguimiento de producción (q-plant) | | |
| **Bodegas e inventarios** | DOC – 09 | Documento físico con los reportes de inventarios | Falta de contraseñas y controles para el manejo de las impresoras y fotocopiadoras. | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados |
| | DOC – 09 | Documento físico con los reportes de inventarios | Falta de políticas para el adecuado manejo de documentos impresos, con información importante | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. |
| **Bodegas e inventarios** | DOC – 10 | Kardex de mercancía en almacén | Falta de control de acceso al archivo digital.. | Filtraciones de información y accesos no autorizados al archivo digital. |
| | DOC – 10 | Kardex de mercancía en almacén | Falta de bloqueo contra escritura y/o lectura del archivo | Lectura y/o modificación de los datos que contiene el documento del Kardex, por parte de personas no autorizadas. |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | HW - 13 | PC's en las bodegas y almacenes | Falta de control de acceso al lugar donde se encuentra las PC's | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. |
| | | | Falta de bitácoras de acceso a la PC. | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de Planificación por parte de cada usuario. |
| | | | Falta de correcta identificación de usuarios y contraseñas para acceder a la PC. | Filtraciones de información y accesos no autorizados a las PC's de la oficina de planificación por parte de usuarios no autorizados o ajenos a la empresa. |
| | | | Falta de seguridad de la red interna median la cual están interconectadas las PC's | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización. |
| **Bodegas e inventarios** | HW – 14 | Cintas de back up | Falta de control de acceso al lugar donde se encuentra guardadas las cintas. | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Poca higiene en el lugar donde se guarda las cintas. | Deterioro permanente de las cintas. |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | HW – 15 | Dispositivo (robot) para generar back ups | Falta de control de acceso al lugar donde se encuentra el robot. | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Falta de control para el manejo del robot. | Manejo del robot por parte de personas ajenas a la empresa o sin autorización |
| **Bodegas e inventarios** | HW – 16 | Pantalla táctil con aplicación Q-Plant | Falta de correcta identificación de usuarios y contraseñas para acceder a la pantalla. | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. |
| | | | Ubicación inadecuada de la pantalla. | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación |
| **Bodegas e inventarios** | AF – 07 | Cámaras de seguridad | Falta de control de acceso a la central de vigilancia donde se encuentra los monitores y demás equipos donde se ven las imágenes de las cámaras. | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. |
| | | | Ubicación inadecuada de las cámaras. | Facilidad de manipulación de las cámaras por parte de personal no autorizado. |
| **Bodegas e inventarios** | AF - 08 | Impresoras | Falta de contraseñas y controles para el manejo de las impresoras. | Facilidad de acceso y manejo de la impresora del área de planificación por parte de personas sin autorización y ajenas al subproceso o a la empresa. |
| | | | Falta de bitácoras de seguimiento del manejo de la impresora. | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de Planificación por parte de cada usuario. |

| Subproceso | Id | Activo | Vulnerabilidades | Amenazas |
|---|---|---|---|---|
| **Bodegas e inventarios** | SW – 07 | Correo electrónico | Falta de Antivirus y Antispam para contrarrestar los virus que puedan contener los correos maliciosos. | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. |
| | | | Mala configuración de los firewall | Accesos maliciosos mediante correos electrónicos. |
| | | | Falta de protección de los servidores de correo electrónico | Ataques a los servidores de correo electrónico por parte de personas ajenas a la organización. |
| | | | Acceso remoto al correo electrónico poco seguro | Acceso al correo electrónico de los usuarios del área de planificación por parte de personas no autorizadas. |
| | | | Falta de políticas para el correcto uso del correo electrónico de la empresa. | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. |
| **Bodegas e inventarios** | SW - 08 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Falta de control de acceso al lugar donde se encuentra guardados los medios de almacenamiento. | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. |

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 3: Matriz de Riesgos

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

- **Identificación de riesgos y análisis de impacto de los activos del subproceso de Planificación:**

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 01 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas ajenas a la empresa. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones así como el daño que causara la filtración de información confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información sobre los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de usuarios inadecuados. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Pérdida o daño a la información o al sistema que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos por parte de hackers | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. | Pérdida o daño a la información o al sistema que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 02 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos , por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la<br><br>Reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de<br><br>Oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de usuarios inadecuados. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Pérdida o daño a la información o al sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de hackers. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de<br>oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 01 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Media | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Media | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Media | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre las listas de pedidos de materiales para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Media | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 03 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas ajenas a la empresa. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | impacto cualitativo alta ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de usuarios inadecuados. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de hackers. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de los usuarios debido a desconocimiento. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 02 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre las listas de pedidos de materiales para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Alta | Significativo | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 04 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a lareputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa , por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial.. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste deoportunidad por no poder utilizar estos recursos para la empresa. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida deoportunidades de negocio. | impacto cualitativo muy alto ya que es difícil medir el coste deoportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de usuarios inadecuados. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida deoportunidades de negocio. | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Pérdida o daño a la información o al sistema, que maneja las ordenes de producción de la empresa, por parte de hackers. | Alta | Catastrófico | Daño ocasionado a lo clientes mediante la distribución de productos de poca calidad o dañinos | impacto cualitativo muy alto ya que es difícil medir el coste deoportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja las ordenes de producción de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 03 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre las órdenes de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 05 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajos de producción de la empresa , por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial.. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de usuarios inadecuados. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Pérdida o daño a la información o al sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de hackers. | Alta | Catastrófico | Daño ocasionado a lo clientes mediante la distribución de productos de poca calidad o dañinos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algun robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 04 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre la ejecución de las ordenes de producción, por parte personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre la ejecución de las ordenes de producción, por parte personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre la ejecución de las ordenes de producción, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre la ejecución de las ordenes de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 06 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas ajenas a la empresa. | Alta | Importante | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de usuarios inadecuados. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de los usuarios debido a desconocimiento.. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW - 01 | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo medio porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de Planificación por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| | Filtraciones de información y accesos no autorizados a las PC's de la oficina de planificación por parte de usuarios no autorizados o ajenos a la empresa. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización.. | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones así como el daño que causara la filtración de información confidencial. |
| HW - 02 | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de las cintas con información sobre planificación por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Deterioro permanente de las cintas. | Perdida de información del proceso de planeación contenida en las cintas de back up. | Media | Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estas cintas. | impacto medio ya que no se puede medir el problema que causara para la empresa la perdida de estas cintas de back up. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW - 03 | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Manejo del robot por parte de personas ajenas a la empresa o sin autorización | Robo de información sobre planificación mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas.. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| HW - 04 | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación | Robo de información sobre las ordenes de proceso y ordenes de trabajo, por parte de personas no autorizadas. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| AF - 01 | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. | Robo de los videos registrados con las camaras de seguridad del área de planificación, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio.. |
| | Facilidad de manipulación de las camaras por parte de personal no autorizado. | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de Planificación. | Baja | Menor | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo bajo ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| AF - 02 | Facilidad de acceso y manejo de la impresora del área de planificación por parte de personas sin autorización y ajenas al subproceso o a la empresa. | Robo de la información contenida en los documentos importantes del área de planificación, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de Planificación por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de planificación. | Baja | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| SW - 01 | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. | Robo de la información contenida en las computadoras del área de Planificación y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Accesos maliciosos mediante correos electrónicos. | Robo de la información contenida en las computadoras del área de Planificación, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Acceso al correo electronico de los usuarios del área de planificación por parte de personas no autorizadas. | Robo de la información contenida en los correos electrónicos del personal del área de Planificación, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de planificación. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SW - 02 | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. | Robo de los medios de almacenamiento con información sobre planificación por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |

- **Identificación de riesgos y análisis de impacto de los activos del subproceso de Manufactura:**

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 07 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas ajenas a la empresa. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencia |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial.. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de usuarios inadecuados. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento pudiendo causar daños al sistema o a la información. | Pérdida o daño a la información o al sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 05 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre la trazabilidad de las transacciones internas de los materiales, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre la trazabilidad de las transacciones internas de los materiales, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre la trazabilidad de las transacciones internas de los materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre la trazabilidad de las transacciones internas de los materiales, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 08 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el registro de cada consumo de materia prima o material intermedio durante el proceso de manufactura, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas ajenas a la empresa. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de usuarios inadecuados. | Alta | Importante | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | impacto cualitativa alto ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de los usuarios debido a desconocimiento.. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 06 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre los consumos que se hacen de todos los materiales durante la manufactura, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 09 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas ajenas a la empresa. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de usuarios inadecuados. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativa alto ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja la declaración de los productos terminados, por parte de los usuarios debido a desconocimiento. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 10 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de usuarios inadecuados. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativa muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 11 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo muy alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de usuarios inadecuados. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativa muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 12 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información muy confidencial. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas ajenas a la empresa. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información confidencial. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información confidencial. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de usuarios inadecuados. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información confidencial. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre las unidades de medida de la materia prima y de las cantidades de producción por parte de personas sin autorización. | Media | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos y aplicación, para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de los usuarios debido a desconocimiento. | Media | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 13 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas ajenas a la empresa. | Alta | Importante | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de usuarios inadecuados. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW – 05 | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de manufactura por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| | Filtraciones de información y accesos no autorizados a las PC's de la oficina de manufactura por parte de usuarios no autorizados o ajenos a la empresa. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización.. | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones así como el daño que causara la filtración de información confidencial. |
| HW - 06 | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de las cintas con información sobre la manufactura por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Deterioro permanente de las cintas. | Perdida de información del proceso de planeación contenida en las cintas de back up. | Media | Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estas cintas. | Impacto medio ya que no se puede medir el problema que causara para la empresa la perdida de estas cintas de back up. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW - 07 | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Manejo del robot por parte de personas ajenas a la empresa o sin autorización | Robo de información sobre manufactura mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| HW - 08 | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación | Robo de información sobre el proceso de manufactura en ejecución, por parte de personas no autorizadas. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| AF - 03 | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. | Robo de los videos registrados con las camaras de seguridad del área de manufactura, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio.. |
| | Facilidad de manipulación de las camaras por parte de personal no autorizado. | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de manufactura. | Baja | Menor | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación | Impacto cualitativo bajo ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| AF - 04 | Facilidad de acceso y manejo de la impresora del área de manufactura por parte de personas sin autorización y ajenas al subproceso o a la empresa. | Robo de la información contenida en los documentos importantes del área de manufactura, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de manufactura por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de manufactura. | Baja | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| SW - 03 | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. | Robo de la información contenida en las computadoras del área de Planificación y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Accesos maliciosos mediante correos electrónicos. | Robo de la información contenida en las computadoras del área de Planificación, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Acceso al correo electronico de los usuarios del área de manufactura por parte de personas no autorizadas. | Robo de la información contenida en los correos electrónicos del personal del área de manufactura, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de manufactura. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| SW - 04 | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. | Robo de los medios de almacenamiento con información sobre el proceso de manufactura por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |

- **Identificación de riesgos y análisis de impacto de los activos del subproceso de Calidad:**

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 14 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es dificil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre los procesos de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de usuarios inadecuados. | Alta | Catastrófico | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre los procesos de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Daño ocasionado a lo clientes mediante la distribución de productos de poca calidad o dañinos | Impacto cualitativo muy alto porque es difícil de medir las consecuencias negativas que traerá el disgusto del cliente |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite controlar los proceso de calidad, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algun robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 07 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre los resultados obtenidos en las pruebas de calidad de los productos, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 15 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas ajenas a la empresa. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es dificil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de usuarios inadecuados. | Alta | Mayor | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Daño ocasionado a lo clientes mediante la distribución de productos de poca calidad o dañinos | Impacto cualitativo muy alto porque es difícil de medir las consecuencias negativas que traerá el disgusto del cliente |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algun robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 08 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS - 16 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas ajenas a la empresa. | Alta | Importante | Retrasos en los procesos de producción, pérdida de pedidos, impacto en la calidad del producto, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos de en producción, las fallas en la calidad, etc. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de usuarios inadecuados. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW – 09 | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las oficinas de calidad por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| | Filtraciones de información y accesos no autorizados a las PC's de la oficina de calidad por parte de usuarios no autorizados o ajenos a la empresa. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización.. | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones así como el daño que causara la filtración de información confidencial. |
| HW - 10 | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de las cintas con información sobre la calidad de los productos por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Deterioro permanente de las cintas. | Perdida de información del proceso de calidad contenida en las cintas de back up. | Media | Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estas cintas. | Impacto medio ya que no se puede medir el problema que causara para la empresa la perdida de estas cintas de back up. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW – 11 | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Manejo del robot por parte de personas ajenas a la empresa o sin autorización | Robo de información sobre calidad mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas.. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| HW – 12 | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación | Robo de información sobre la calidad de los productos que se están fabricando, por parte de personas no autorizadas. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| AF – 05 | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. | Robo de los videos registrados con las camaras de seguridad del área de calidad, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso.. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio.. |
| | Facilidad de manipulación de las camaras por parte de personal no autorizado. | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de calidad. | Baja | Menor | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación | Impacto cualitativo bajo ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| AF – 06 | Facilidad de acceso y manejo de la impresora del área de calidad por parte de personas sin autorización y ajenas al subproceso o a la empresa. | Robo de la información contenida en los documentos importantes del área de calidad, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las impresoras de las oficinas de calidad por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de calidad.. | Baja | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| SW - 05 | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. | Robo de la información contenida en las computadoras del área de calidad y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Accesos maliciosos mediante correos electrónicos. | Robo de la información contenida en las computadoras del área de calidad, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Acceso al correo electronico de los usuarios del área de calidad por parte de personas no autorizadas. | Robo de la información contenida en los correos electrónicos del personal del área de calidad, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de calidad. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| SW - 06 | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. | Robo de los medios de almacenamiento con información sobre el proceso de calidad por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |

- **Identificación de riesgos y análisis de impacto de los activos del subproceso de Bodegas e inventarios:**

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 17 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas ajenas a la empresa. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre los inventarios tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Retrasos en los procesos de bodegas, pérdida y error en la entrega de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los errores y perdidas en la entrega de los pedidos |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de usuarios inadecuados. | Alta | Importante | Retrasos en los procesos de bodegas, pérdida y error en la entrega de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los errores y perdidas en la entrega de los pedidos |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre los inventarios tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitatitvo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC - 09 | Deterioro permanente de los documentos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estos documentos. | Impacto medio ya que los documentos pueden volver a ser impresos a través de la aplicación. |
| | Acceso a los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de los documentos y su información, sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Acceso a las copias de los documentos por parte de personas ajenas a la empresa o por usuarios inadecuados | Robo de las copias los documentos y su información, sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo de las impresoras/fotocopiadoras del área por parte de usuarios inadecuados. | Robo de la información contenida en los documentos sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Manejo inadecuado de los documentos y/o sus copias por parte de los usuarios de la empresa debido al desconocimiento. | Pérdida o daño a los documentos que contienen la información sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 18 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes o puntos de distribución, por parte de personas sin autorización. | Alta | Mayor | Posible impacto en la imagen de la empresa ante terceros. | Impacto cualitativo muy alto debido a la pérdida de credibilidad en los mercados, daño a la reputación de la empresa, pérdida de confianza por parte de los clientes y los proveedores. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas ajenas a la empresa. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Retrasos en los procesos de entrega y distribución, pérdida de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en la entrega y distribución de pedidos. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de usuarios inadecuados. | Alta | Mayor | Retrasos en los procesos de entrega y distribución, pérdida de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo muy alto porque es difícil medir el daño que causara a la empresa los retrasos de en la entrega y distribución de pedidos. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo muy alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algun robo o daño a la información o a la aplicación. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 19 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas ajenas a la empresa. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Retrasos en los procesos de traslados internos de materia prima o productos, perdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los retrasos en los traslados internos. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de usuarios inadecuados. | Alta | Importante | Retrasos en los procesos de entrega y distribución, pérdida de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los errores y perdidas en la entrega de los pedidos |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| SIS – 20 | Filtraciones de información y accesos no autorizados el sistema. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Accesos de personas no autorizadas al sistema e intercepción de la red | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas ajenas a la empresa. | Alta | Importante | Retrasos en los procesos de bodegas, pérdida y error en la entrega de pedidos, pérdida de oportunidades de negocio. | impacto cualitativo alto porque es difícil medir el daño que causara a la empresa los errores y perdidas en la entrega de los pedidos |
| | Acceso de personas ajenas a la empresa que pueden robar información. | Robo de la información, sobre el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Acceso al sistema por parte de usuarios inadecuados que no deberían tener dicho acceso. | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de usuarios inadecuados. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada. | Robo de la información, sobre el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Uso inadecuado de la aplicación y sus información por parte de los usuarios debido a desconocimiento | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Desconocimiento sobre los intentos de accesos y acciones a la aplicación por parte de los usuarios. | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| DOC – 10 | Filtraciones de información y accesos no autorizados al archivo digital. | Robo de la información y manipulación maliciosa del archivo digital, que contiene toda la información de las mercancías como cantidad, valor de medida, precio, etc., por parte de personas sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Lectura y/o modificación de los datos que contiene el documento del Kardex, por parte de personas no autorizadas. | Robo de la información y manipulación maliciosa del archivo digital, que contiene toda la información de las mercancías como cantidad, valor de medida, precio, etc., por parte de personas sin autorización. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de<br>oportunidad por no poder utilizar estos recursos para la empresa. |
| HW – 13 | Acceso a las oficinas donde se encuentran las PC's, por parte de personas ajenas a la empresa o por personal no autorizado. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros. | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información no tan relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las PC's de las bodegas por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| | Filtraciones de información y accesos no autorizados a las PC's de las bodegas por parte de usuarios no autorizados o ajenos a la empresa. | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| | Interceptación de la red de la empresa por parte de personas ajenas al negocio o usuarios sin autorización. | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo alto porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones así como el daño que causara la filtración de información confidencial. |
| HW – 14 | Acceso a las cintas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Robo de las cintas con información sobre las bodegas y almacenes, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Deterioro permanente de las cintas. | Perdida de información del proceso de calidad contenida en las cintas de back up. | Media | Significativo | Perdidas ocasionadas por la indisponibilidad de la información contenida en estas cintas. | Impacto medio ya que no se puede medir el problema que causara para la empresa la perdida de estas cintas de back up. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| HW – 15 | Acceso al robot por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Manejo del robot por parte de personas ajenas a la empresa o sin autorización | Robo de información sobre bodegas e inventarios mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas. | Media | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| HW – 16 | Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados. | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alto ya que es difícil medir el coste de<br><br>oportunidad por no poder utilizar estos recursos para la empresa. |
| | Visibilidad de lo que muestra las pantallas por parte de personas no autorizadas o daños graves a las pantallas debido a su mala ubicación | Robo de información sobre el almacenaje de los productos terminados, por parte de personas no autorizadas. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| AF – 07 | Fácil acceso a la central de vigilancia por parte de personas ajenas a la empresa o por usuarios no autorizados. | Robo de los videos registrados con las camaras de seguridad del área de bodegas e inventarios, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio.. |
| | Facilidad de manipulación de las camaras por parte de personal no autorizado. | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de bodegas e inventarios. | Baja | Menor | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación | Impacto cualitativo bajo ya que no considera muy indispensable para la continuidad del negocio. |

| Id | Amenazas | Riesgos | Prioridad | Impacto | | |
|---|---|---|---|---|---|---|
| | | | | Gravedad | Tipo | descripción |
| AF – 08 | Facilidad de acceso y manejo de la impresora del área de bodegas por parte de personas sin autorización y ajenas al subproceso o a la empresa. | Robo de la información contenida en los documentos importantes del área de bodegas e inventarios, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Desconocimiento sobre los intentos de accesos y acciones en las impresoras del área de bodegas por parte de cada usuario. | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de bodegas e inventarios. | Baja | Significativo | Falta de captura y demanda contra el autor del daño o perjuicio a la aplicación. | Impacto cualitativo medio ya que no considera muy indispensable para la continuidad del negocio. |
| SW - 07 | Penetración y propagación de virus y spam en la red interna de la empresa mediante emails maliciosos. | Robo de la información contenida en las computadoras del área de bodegas e inventarios, y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Pérdidas ocasionadas por la indisponibilidad de la aplicación y servicios informáticos | impacto cualitativo alta ya que es difícil medir el coste de oportunidad por no poder utilizar estos recursos para la empresa. |
| | Accesos maliciosos mediante correos electrónicos. | Robo de la información contenida en las computadoras del área de bodegas e inventarios, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante.. |
| | Ataques a los servidores de correo electronico por parte de personas ajenas a la organización. | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Horas de trabajo invertidas en las reparaciones y reconfiguraciones de los equipos y redes | Impacto cualitativo medio porque es difícil medir el retraso y perdida de tiempo que causara estas reparaciones. |
| | Acceso al correo electronico de los usuarios del área de bodegas por parte de personas no autorizadas. | Robo de la información contenida en los correos electrónicos del personal del área de bodegas e inventarios, por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |
| | Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento. | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de bodegas e inventarios. | Alta | Mayor | Divulgación de información personal privada de los usuarios de la empresa, clientes, proveedores, etc. | Impacto cualitativo alto ya que es difícil medir el daño que causara en la empresa el descontento por parte de sus clientes y/o proveedores al ser revelada su información privada. |
| SW - 08 | Fácil acceso a lugar donde se guardan los medios de almacenamiento por parte de personas no autorizadas o ajenas a la empresa. | Robo de los medios de almacenamiento con información sobre el proceso de bodegas e inventarios por parte de personas no autorizadas. | Alta | Mayor | Robo de información confidencial y su posible revelación a terceros | Impacto cualitativo alto porque es difícil medir el daño que causara a la empresa la divulgación de información relevante. |

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 4:

# Tratamiento de riesgos

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

- **Análisis de tratamiento de riesgos de los activos del subproceso de Planificación:**

| Id | Activo | Riesgos | Prioridad | Gravedad de impacto | Tratamiento |
|---|---|---|---|---|---|
| SIS - 01 | Interfaz para modificar, dar de alta y baja materiales | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas ajenas a la empresa. | Alta | Mayor | Eliminar |
| | | Robo de la información sobre los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de usuarios inadecuados. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos por parte de hackers | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS - 02 | Interfaz para administrar pedidos de materiales | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos , por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los recursos y materiales que usa la empresa para la fabricación de sus productos, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de hackers. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja los pedidos de materiales y los programas de producción que usa la empresa para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC - 01 | Documento físico con lista de pedido de materiales | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Transferir |
| | | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Media | Significativo | Transferir |
| | | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Media | Significativo | Mitigar |
| | | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Media | Significativo | Mitigar |
| | | Pérdida o daño a los documentos que contienen la información sobre las listas de pedidos de materiales para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS - 03 | Interfaz de mantenimiento de productos | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas ajenas a la empresa. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de usuarios inadecuados. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de hackers. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el catalogo de productos que fabrica la empresa, por parte de los usuarios debido a desconocimiento. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 02 | Interfaz de mantenimiento de Ordenes de Producción | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Transferir |
| | | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Significativo | Transferir |
| | | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Significativo | Mitigar |
| | | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Significativo | Mitigar |
| | | Pérdida o daño a los documentos que contienen la información sobre las listas de pedidos de materiales para la fabricación de sus productos, por parte de los usuarios debido a desconocimiento. | Alta | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 04 | Interfaz de mantenimiento de productos | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa , por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de producción de la empresa, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja las ordenes de producción de la empresa, por parte de hackers. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja las ordenes de producción de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 03 | Documento físico con reportes de las órdenes de producción. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Transferir |
| | | Robo de los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Mayor | Transferir |
| | | Robo de las copias los documentos y su información, sobre la listas de pedidos de materiales para la producción, por parte personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los documentos sobre la lista de pedidos de materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre las órdenes de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 05 | Sistema de mantenimiento de Ordenes de trabajos de Producción | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajos de producción de la empresa , por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja las ordenes de trabajo de producción de la empresa, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja las órdenes de trabajo de producción de la empresa, por parte de hackers. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja las órdenes de trabajo de producción de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 04 | Documento físico con reportes de las órdenes de producción. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Transferir |
| | | Robo de los documentos y su información, sobre la ejecución de las ordenes de producción, por parte personas sin autorización. | Alta | Mayor | Transferir |
| | | Robo de las copias los documentos y su información, sobre la ejecución de las ordenes de producción, por parte personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los documentos sobre la ejecución de las ordenes de producción, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre la ejecución de las ordenes de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 06 | Sistema de seguimiento de producción | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de los usuarios debido a desconocimiento.. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| HW – 01 | PC's en el área de Planificación | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Mitigar |
| | | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| HW- 02 | Cintas de back up | Robo de las cintas con información sobre planificación por parte de personas no autorizadas. | Alta | Mayor | Transferir |
| | | Perdida de información del proceso de planeación contenida en las cintas de back up. | Media | Significativo | Transferir |

| | | | | | |
|---|---|---|---|---|---|
| HW – 03 | Dispositivo (robot) para generar back ups | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Mitigar |
| | | Robo de información sobre planificación mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas.. | Media | Mayor | Eliminar |
| HW – 04 | Pantalla táctil con aplicación Q-Plant | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| | | Robo de información sobre las órdenes de proceso y ordenes de trabajo, por parte de personas no autorizadas. | Alta | Importante | Mitigar |
| AF – 01 | Cámaras de seguridad | Robo de los videos registrados con las camaras de seguridad del área de planificación, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Mitigar |
| | | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de Planificación. | Baja | Menor | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| AF – 02 | Impresoras | Robo de la información contenida en los documentos importantes del área de manufactura, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de manufactura. | Baja | Significativo | Mitigar |
| SW – 01 | Correo electronico | Robo de la información contenida en las computadoras del área de Planificación y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las computadoras del área de Planificación, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los correos electrónicos del personal del área de manufactura, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de manufactura. | Alta | Mayor | Eliminar |
| SW – 02 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Robo de los medios de almacenamiento con información sobre el proceso de manufactura por parte de personas no autorizadas. | Alta | Mayor | Transferir |

- **Analisis de tratamiento de riesgos de los activos del subproceso de Manufactura:**

| Id | Activo | Riesgos | Prioridad | Gravedad de impacto | Tratamiento |
|---|---|---|---|---|---|
| SIS - 07 | Interfaz de trazabilidad de materiales en Producción | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas ajenas a la empresa. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de usuarios inadecuados. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de las transacciones internas de materiales que se dan en el proceso de producción, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 05 | Documento físico con reportes de la trazabilidad de materiales en un programa de producción | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Mitigar |
| | | Robo de los documentos y su información, sobre la trazabilidad de las transacciones internas de los materiales, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de las copias los documentos y su información, sobre la trazabilidad de las transacciones internas de los materiales, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información contenida en los documentos sobre la trazabilidad de las transacciones internas de los materiales, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre la trazabilidad de las transacciones internas de los materiales, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 08 | Interfaz de declaración de consumo de materiales | Robo de la información y manipulación maliciosa del sistema, que maneja el registro de cada consumo de materia prima o material intermedio durante el proceso de manufactura, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de planificación, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de planificación, por parte de los usuarios debido a desconocimiento.. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 06 | Documento físico con reportes de los consumos de materiales | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Mitigar |
| | | Robo de los documentos y su información, sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de las copias los documentos y su información, sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información contenida en los documentos sobre los consumos que se hacen de todos los materiales durante la manufactura, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre los consumos que se hacen de todos los materiales durante la manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 09 | Interfaz de declaración de producto terminado | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas ajenas a la empresa. | Media | Mayor | Eliminar |
| | | Robo de la información, sobre la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja la declaración de los productos terminados, por parte de usuarios inadecuados. | Media | Mayor | Eliminar |
| | | Robo de la información, sobre la declaración de los productos terminados, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja la declaración de los productos terminados, por parte de los usuarios debido a desconocimiento. | Media | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 10 | Interfaz de ejecución de Orden de Proceso | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre la ejecución del la orden de proceso de manufactura, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite iniciar la ejecución del la orden de proceso de manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 11 | Interfaz de Surtimiento de materiales a producción | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre el surtimiento de materias primas para la fabricación de determinado producto, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite realizar el surtimiento de materias primas para la fabricación de determinado producto, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 12 | Interfaz de consulta y borrado de RS's y creación de unidades de medida para las materias primas | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas ajenas a la empresa. | Media | Mayor | Eliminar |
| | | Robo de la información, sobre las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de usuarios inadecuados. | Media | Mayor | Eliminar |
| | | Robo de la información, sobre las unidades de medida de la materia prima y de las cantidades de producción por parte de personas sin autorización. | Media | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite modificar las unidades de medida de la materia prima y de las cantidades de producción, por parte de los usuarios debido a desconocimiento. | Media | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 13 | Sistema de seguimiento de producción | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de manufactura, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de manufactura, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| HW – 05 | PC's en planta | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Eliminar |
| | | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| HW- 06 | Cintas de back up | Robo de las cintas con información sobre la manufactura por parte de personas no autorizadas. | Alta | Mayor | Transferir |
| | | Perdida de información del proceso de planeación contenida en las cintas de back up. | Media | Significativo | Transferir |

| | | | | | |
|---|---|---|---|---|---|
| HW – 07 | Dispositivo (robot) para generar back ups | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Mitigar |
| | | Robo de información sobre manufactura mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas. | Media | Mayor | Eliminar |
| HW – 08 | Pantalla táctil con aplicación Q-Plant | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| | | Robo de información sobre el proceso de manufactura en ejecución, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| AF – 03 | Cámaras de seguridad | Robo de los videos registrados con las camaras de seguridad del área de manufactura, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Mitigar |
| | | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de manufactura. | Baja | Menor | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| AF – 04 | Impresoras | Robo de la información contenida en los documentos importantes del área de manufactura, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de manufactura. | Baja | Significativo | Mitigar |
| SW – 03 | Correo electronico | Robo de la información contenida en las computadoras del área de Planificación y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las computadoras del área de Planificación, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los correos electrónicos del personal del área de manufactura, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de manufactura. | Alta | Mayor | Eliminar |
| SW – 04 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Robo de los medios de almacenamiento con información sobre el proceso de manufactura por parte de personas no autorizadas. | Alta | Mayor | Transferir |

- **Analisis de tratamiento de riesgos de los activos del subproceso de Calidad:**

| Id | Activo | Riesgos | Prioridad | Gravedad de impacto | Tratamiento |
|---|---|---|---|---|---|
| SIS - 14 | Interfaz de control del procesos de Calidad | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Transferir |
| | | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas ajenas a la empresa. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre los procesos de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de usuarios inadecuados. | Alta | Catastrófico | Eliminar |
| | | Robo de la información, sobre los procesos de calidad, por parte de personas sin autorización. | Alta | Catastrófico | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite controlar los proceso de calidad, por parte de los usuarios debido a desconocimiento. | Alta | Catastrófico | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 07 | Documento físico con reportes de resultados de los controles de calidad | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Mitigar |
| | | Robo de los documentos y su información, sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de las copias los documentos y su información, sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información contenida en los documentos sobre los resultados obtenidos en las pruebas de calidad de los productos, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre los resultados obtenidos en las pruebas de calidad de los productos, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 15 | Interfaz de gestión de calidad | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas ajenas a la empresa. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite controlar los proceso de calidad, por parte de usuarios inadecuados. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre los niveles de calidad que tendrán los productos, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite gestionar los niveles de calidad que tendrán los productos, por parte de los usuarios debido a desconocimiento. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Importante | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 08 | Documento físico con los niveles de calidad que tendrán los productos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Mitigar |
| | | Robo de los documentos y su información, sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de las copias los documentos y su información, sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información contenida en los documentos sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre los distintos niveles de calidad que se le han asignado a cada diferente producto que produce la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 16 | Sistema de seguimiento de producción (q-plant) | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de calidad, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de calidad, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| HW – 09 | PC's en planta | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Mitigar |
| | | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las PC's, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| HW- 10 | Cintas de back up | Robo de las cintas con información sobre la calidad de los productos por parte de personas no autorizadas. | Alta | Mayor | Transferir |
| | | Perdida de información del proceso de calidad contenida en las cintas de back up. | Media | Significativo | Transferir |

| | | | | | |
|---|---|---|---|---|---|
| HW – 11 | Dispositivo (robot) para generar back ups | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Mitigar |
| | | Robo de información sobre calidad mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas.. | Media | Mayor | Eliminar |
| HW – 12 | Pantalla táctil con aplicación Q-Plant | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| | | Robo de información sobre la calidad de los productos que se están fabricando, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| AF – 05 | Cámaras de seguridad | Robo de los videos registrados con las camaras de seguridad del área de calidad, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso.. | Media | Significativo | Mitigar |
| | | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de calidad. | Baja | Menor | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| AF – 06 | Impresoras | Robo de la información contenida en los documentos importantes del área de calidad, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de calidad.. | Baja | Significativo | Mitigar |
| SW – 05 | Correo electronico | Robo de la información contenida en las computadoras del área de calidad y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las computadoras del área de calidad, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los correos electrónicos del personal del área de calidad, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de calidad. | Alta | Mayor | Eliminar |
| SW – 06 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Robo de los medios de almacenamiento con información sobre el proceso de calidad por parte de personas no autorizadas. | Alta | Mayor | Eliminar |

- **Analisis de tratamiento de riesgos de los activos del subproceso de Bodegas e inventarios:**

| Id | Activo | Riesgos | Prioridad | Gravedad de impacto | Tratamiento |
|---|---|---|---|---|---|
| SIS - 17 | Interfaz de generación de reportes de inventarios | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre los inventarios tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre los inventarios tanto de materias primas como de productos terminados que tiene la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite generar reportes del inventario tanto de materias primas como de productos terminados que tiene la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 09 | Documento físico con los niveles de calidad que tendrán los productos. | Falta de disponibilidad de la información contenida en el documento, en el momento que sea requerida. | Media | Poco Significativo | Mitigar |
| | | Robo de los documentos y su información, sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de las copias los documentos y su información, sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información contenida en los documentos sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a los documentos que contienen la información sobre los distintos reportes de inventarios de las bodegas y almacenes de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 18 | Interfaz de entrega de salida de productos terminados | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes o puntos de distribución, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas ajenas a la empresa. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de usuarios inadecuados. | Alta | Mayor | Eliminar |
| | | Robo de la información, sobre la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes o puntos de distribución, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite gestionar la entrega de cierta cantidad de productos para que vayan a los almacenes, por parte de personas ajenas a la empresa. | Alta | Mayor | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 19 | Interfaz para traslado de materias primas y productos entre plantas | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que permite registrar el traslado de materias primas o productos terminados entre almacenes de la empresa, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| SIS – 20 | Sistema de seguimiento de producción (q-plant) | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas ajenas a la empresa. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de usuarios inadecuados. | Alta | Importante | Eliminar |
| | | Robo de la información, sobre el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Pérdida o daño a la información o al sistema, que maneja el seguimiento de la producción en la etapa de bodegas e inventarios, por parte de los usuarios debido a desconocimiento. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo o daño a la información o a la aplicación. | Media | Significativo | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| DOC – 10 | Kardex de mercancía en almacén | Robo de la información y manipulación maliciosa del archivo digital, que contiene toda la información de las mercancías como cantidad, valor de medida, precio, etc., por parte de personas sin autorización. | Alta | Importante | Eliminar |
| | | Robo de la información y manipulación maliciosa del archivo digital, que contiene toda la información de las mercancías como cantidad, valor de medida, precio, etc., por parte de personas sin autorización. | Alta | Importante | Eliminar |
| HW – 13 | PC's en las bodegas y almacenes | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información o daño a las PC's. | Media | Importante | Mitigar |
| | | Robo de la información contenida en las PC's y manipulación maliciosa de éstas, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las PC’s, por parte de personas sin autorización. | Alta | Mayor | Eliminar |
| HW – 14 | Cintas de back up | Robo de las cintas con información sobre las bodegas y almacenes, por parte de personas no autorizadas. | Alta | Mayor | Transferir |
| | | Perdida de información del proceso de calidad contenida en las cintas de back up. | Media | Significativo | Transferir |

| | | | | | |
|---|---|---|---|---|---|
| HW – 15 | Dispositivo (robot) para generar back ups | Manipulación maliciosa del robot para dañarlo, por parte de personas no autorizadas. | Media | Importante | Mitigar |
| | | Robo de información sobre bodegas e inventarios mediante el uso del dispositivo para realizar copias de las cintas de back up, por parte de personas no autorizadas. | Media | Mayor | Eliminar |
| HW – 16 | Pantalla táctil con aplicación Q-Plant | Manipulación maliciosa de la pantalla para dañarla o robar información, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| | | Robo de información sobre el almacenaje de los productos terminados, por parte de personas no autorizadas. | Alta | Importante | Eliminar |
| AF – 07 | Cámaras de seguridad | Robo de los videos registrados con las camaras de seguridad del área de bodegas e inventarios, por parte de personas no autorizadas para no dejar evidencias de algún acto malicioso. | Media | Significativo | Mitigar |
| | | Manipulación de las cámaras por parte de personas no autorizadas con el fin de mover su ángulo de filmación o desconectarlas para evitar que se filme algún acto malicioso en el área de bodegas e inventarios. | Baja | Menor | Mitigar |

| | | | | | |
|---|---|---|---|---|---|
| AF – 08 | Impresoras | Robo de la información contenida en los documentos importantes del área de bodegas e inventarios, mediante la realización de fotocopiado por parte de usuarios sin autorización. | Alta | Importante | Eliminar |
| | | Imposibilidad de identificar al o a los usuarios culpables de algún robo de información mediante el fotocopiado de documentos privados del área de bodegas e inventarios. | Baja | Significativo | Mitigar |
| SW – 07 | Correo electronico | Robo de la información contenida en las computadoras del área de bodegas e inventarios, y/o daño a estas, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en las computadoras del área de bodegas e inventarios, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información o daño a los servidores de correo electronico, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Robo de la información contenida en los correos electrónicos del personal del área de bodegas e inventarios, por parte de personas no autorizadas. | Alta | Mayor | Eliminar |
| | | Perdida o divulgación de información confidencial de la empresa mediante el correo electronico, por parte del personal del área de bodegas e inventarios. | Alta | Mayor | Eliminar |
| SW – 08 | Medios de almacenamiento electrónico portátil (CD/DVD/USB) | Robo de los medios de almacenamiento con información sobre el proceso de bodegas e inventarios por parte de personas no autorizadas. | Alta | Mayor | Transferir |

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 5:

# Controles Planteados

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

- **Controles planteados para tratar los riesgos de los activos del subproceso de Planificación:**

| Id | RN | Cláu. | Control 1 | Control 2 | Control 3 | Control 4 |
|---|---|---|---|---|---|---|
| SIS 01/ SIS 02/ SIS 03/ SIS 04/ SIS 05/ SIS 06. | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | CA | Los usuarios solo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica | Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos. | Las identificaciones automáticas de equipo deben ser consideradas como medios para autenticar conexiones desde locales y equipos específicos. | Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones de negocio. |
| | R3 | ADM | Se deben revisar y probar las aplicaciones del sistema operativo cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad. | - | - | - |
| | R4 | CA | Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. | Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. | Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivos para asegurar la calidad de las mismas. | - |
| | R5 | CA | Debería restringirse y controlarse el uso y asignación de privilegios. | Todos los usuarios deberían disponer un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos. | La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado. | Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida. |
| | R6 | ADM | La implementación de cambios debe ser controlada usando procedimiento formales de cambio. | Debe haber restricciones en los cambios a los paquetes de software. No se recomiendan modificaciones a los paquetes de software, se deberían limitar a cambios necesarios y todos estos debe ser estrictamente controlados. | Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas. | - |
| | R7 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| | R8 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |

| | | | | | | |
|---|---|---|---|---|---|---|
| DOC 01/ DOC 02/ DOC 03/ DOC 04 | R1 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R2 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R3 | CA | Se debería adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento. | - | - | - |
| | R4 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| HW 01 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | - |
| | R3 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R4 | GC | Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito. | Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización. | | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| HW 02 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |
| | R2 | GC | Debería haber procedimientos para la gestión de medios informáticos removibles. | Se deberían Eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales. | - | - |
| HW 03 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | SFA | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - |
| HW 04 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |
| AF 01 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | - | - |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| AF 02 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |
| SW 01 | R1 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática. | - | - |
| | R2 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | - | - | - |
| | R3 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - | - |
| | R4 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y otros. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuó, adecuación y efectividad. | - | - |
| SW 02 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |

- **Controles planteados para tratar los riesgos de los activos del subproceso de Manufactura:**

| Id | RN | Cláu. | Control 1 | Control 2 | Control 3 | Control 4 |
|---|---|---|---|---|---|---|
| SIS 07/ SIS 08/ SIS 09/ SIS 10/ SIS 11/ SIS 12/ SIS 13. | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | CA | Los usuarios solo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica | Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos. | Las identificaciones automáticas de equipo deben ser consideradas como medios para autenticar conexiones desde locales y equipos específicos. | Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones de negocio. |
| | R3 | ADM | Se deben revisar y probar las aplicaciones del sistema operativo cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad. | - | - | - |
| | R4 | CA | Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. | Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. | Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas. | - |
| | R5 | CA | Debería restringirse y controlarse el uso y asignación de privilegios. | Todos los usuarios deberían disponer un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos. | La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado. | Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida. |
| | R6 | ADM | La implementación de cambios debe ser controlada usando procedimiento formales de cambio. | Debe haber restricciones en los cambios a los paquetes de software. No se recomiendan modificaciones a los paquetes de software, se deberían limitar a cambios necesarios y todos estos debe ser estrictamente controlados. | Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas. | - |
| | R7 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| | R8 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |

| | | | | | | |
|---|---|---|---|---|---|---|
| DOC 05/ DOC 06/ | R1 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R2 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R3 | CA | Se debería adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento. | - | - | - |
| | R4 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| HW 05 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | - |
| | R3 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R4 | GC | Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito. | Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización. | | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| HW 06 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |
| | R2 | GC | Debería haber procedimientos para la gestión de medios informáticos removibles. | Se deberían Eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales. | - | - |
| HW 07 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | SFA | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - |
| HW 08 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |
| AF 03 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | - | - |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| AF 04 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |
| SW 03 | R1 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática. | - | - |
| | R2 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | - | - | - |
| | R3 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - | - |
| | R4 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y otros. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuó, adecuación y efectividad. | - | - |
| SW 04 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |

- **Controles planteados para tratar los riesgos de los activos del subproceso de Calidad:**

| Id | RN | Cláu. | Control 1 | Control 2 | Control 3 | Control 4 |
|---|---|---|---|---|---|---|
| SIS 14/ SIS 15/ SIS 16. | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | CA | Los usuarios solo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica | Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos. | Las identificaciones automáticas de equipo deben ser consideradas como medios para autenticar conexiones desde locales y equipos específicos. | Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones de negocio. |
| | R3 | ADM | Se deben revisar y probar las aplicaciones del sistema operativo cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad. | - | - | - |
| | R4 | CA | Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. | Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. | Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas. | - |
| | R5 | CA | Debería restringirse y controlarse el uso y asignación de privilegios. | Todos los usuarios deberían disponer un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos. | La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado. | Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida. |
| | R6 | ADM | La implementación de cambios debe ser controlada usando procedimiento formales de cambio. | Debe haber restricciones en los cambios a los paquetes de software. No se recomiendan modificaciones a los paquetes de software, se deberían limitar a cambios necesarios y todos estos debe ser estrictamente controlados. | Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas. | - |
| | R7 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| | R8 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |

| | | | | | | |
|---|---|---|---|---|---|---|
| DOC 07/ DOC 08/ | R1 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R2 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R3 | CA | Se debería adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento. | - | - | - |
| | R4 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| HW 09 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | - |
| | R3 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R4 | GC | Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito. | Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización. | | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| HW 10 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |
| | R2 | GC | Debería haber procedimientos para la gestión de medios informáticos removibles. | Se deberían Eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales. | - | - |
| HW 11 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | SFA | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - |
| HW 12 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |
| AF 05 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | - | - |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| AF 06 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |
| SW 05 | R1 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática. | - | - |
| | R2 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | - | - | - |
| | R3 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - | - |
| | R4 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y otros. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuó, adecuación y efectividad. | - | - |
| SW 06 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |

- **Controles planteados para tratar los riesgos de los activos del subproceso de Bodegas e inventarios:**

| Id | RN | Cláu. | Control 1 | Control 2 | Control 3 | Control 4 |
|---|---|---|---|---|---|---|
| SIS 17/ SIS 18/ SIS 19/ SIS 20. | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | CA | Los usuarios solo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica | Se deben utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos. | Las identificaciones automáticas de equipo deben ser consideradas como medios para autenticar conexiones desde locales y equipos específicos. | Los requisitos de la política de control de accesos para redes compartidas, sobre todo para las que atraviesan las fronteras de la organización, se deberían basar en los requisitos de las aplicaciones de negocio. |
| | R3 | ADM | Se deben revisar y probar las aplicaciones del sistema operativo cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad. | - | - | - |
| | R4 | CA | Se debería controlar la asignación de contraseñas por medio de un proceso de gestión formal. | Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas. | Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas. | - |
| | R5 | CA | Debería restringirse y controlarse el uso y asignación de privilegios. | Todos los usuarios deberían disponer un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos. | La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado. | Se debería dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida. |
| | R6 | ADM | La implementación de cambios debe ser controlada usando procedimiento formales de cambio. | Debe haber restricciones en los cambios a los paquetes de software. No se recomiendan modificaciones a los paquetes de software, se deberían limitar a cambios necesarios y todos estos debe ser estrictamente controlados. | Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas de información utilizadas. | - |
| | R7 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| | R8 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |

| | | | | | | |
|---|---|---|---|---|---|---|
| DOC 09 | R1 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R2 | GC | La documentación debe ser protegida contra daños o accesos no autorizados. | - | - | - |
| | R3 | CA | Se debería adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento. | - | - | - |
| | R4 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo, adecuación y efectividad. | - | - |
| HW 13 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | - |
| | R3 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R4 | GC | Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito. | Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización. | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| DOC 10 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | - | - | - |
| | R2 | CA | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - | - | - |
| HW 14 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |
| | R2 | GC | Debería haber procedimientos para la gestión de medios informáticos removibles. | Se deberían Eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales. | - | - |
| HW 15 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. |
| | R2 | SFA | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - |
| HW 16 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |
| AF 07 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | - | - |
| | R2 | SFA | El equipo debería situarse y protegerse para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados. | Los equipos deberían mantenerse adecuadamente para asegurar su continua disponibilidad e integridad. | - | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| AF 08 | R1 | CA | Una política de control de acceso debe ser establecida, documentada revisada y debe estar basada en los requerimientos de seguridad y del negocio. | Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuarios. | La gerencia debería establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios. | Las sesiones se deberían desactivar tras un periodo definido de inactividad. |
| | R2 | GC | Los registros de auditoría grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados por un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso. | Los procedimientos para el uso del monitoreo de procesamiento de información, deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente. | Las instalaciones de registros de información deben ser protegidas contra acciones forzosas u accesos no autorizados. | Las actividades del administrador y de los operadores del sistema deben ser registradas. |
| SW 07 | R1 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se debería adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática. | - | - |
| | R2 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | - | - | - |
| | R3 | GC | Se deberían implantar controles para detectar el software malicioso y prevenirse contra él junto a procedimientos adecuados para concientizar a los usuarios. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - | - |
| | R4 | GC | La información implicada con la mensajería electrónica debe ser protegida apropiadamente. | Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y otros. | Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación. | - |
| | R5 | PS | La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. | La política de seguridad debe ser revisada en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuó, adecuación y efectividad. | - | - |
| SW 08 | R1 | SFA | Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas, o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información y recursos de procesamiento de información. | Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso solo al personal autorizado. | La seguridad física para oficinas, despachos y recursos debe ser asignada y aplicada. | - |

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 6:

# Guías de Implementación

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

## Guía de implementación de la cláusula de Política de Seguridad (PS)

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento de la política de seguridad debería contener como mínimo:

- Una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
- El establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
- Un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión de riesgo.
- Una breve explicación de las políticas, principios, normas, y requisitos de conformidad más importantes para la organización.
- Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de información, incluida la comunicación de las incidencias de seguridad.
- Las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta todos los destinatarios en una forma que se apropiada, entendible y accesible.

La política debería tener un propietario que sea responsable del desarrollo, revisión y evaluación de la política de seguridad. La revisión debe incluir oportunidades de evaluación para mejorar la política de seguridad de información de la organización y un acercamiento a la gestión de seguridad de información en respuesta a los cambios del ambiente organizacional, circunstancias del negocio, condiciones legales o cambios en el ambiente técnico.

La revisión de la política de seguridad de información debe tomar en cuenta los resultados de las revisiones de la gestión. Deben existir procedimientos

definidos de la gestión de revisión, incluyendo un calendario o periodo de revisión.

El output para la revisión de la gestión debe incluir información acerca de:

- Mejoras en el alcance de la organización para gestionar seguridad de información y sus procesos.
- Mejoras en los objetivos de control controles.
- Mejoras en la asignación de recursos y/o responsabilidades.

## Guía de implementación de la cláusula de Seguridad física y ambiental (SFA)

Las siguientes pautas deben ser consideradas e implementadas donde sea apropiado para los perímetros de seguridad físicos.

- El perímetro de seguridad debería estar claramente definido y el lugar y fuerza de cada perímetro debe depender de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos.
- El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física (por ejemplo no tendrá zonas que puedan derribarse fácilmente). Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados, por ejemplo, con mecanismos de control, alarmas, rejas, etc. Las ventanas y puertas deben estar cerradas con llave cuando estén desatendidas.
- Se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería permitir solo al personal autorizado.
- Las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno.
- Se debería instalar sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y deben ser regularmente probados.
- Los recursos de procesamiento de información manejadas por la organización deben ser físicamente separadas de las que son manejadas por externos.

Para los controles físicos de entrada deberían considerarse las siguientes pautas:

- Las visitas a las aéreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha y momento de entrada y salida. Los visitantes solo tendrán acceso para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia.
- Se debería controlar y restringir solo al personal autorizado el acceso a la información sensible y al tratamiento de los recursos. Se deberían usar

controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso. Se debería mantener un rastro auditable de todos los accesos, con las debidas medidas de seguridad.

- Se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique.
- Se debe garantizar el acceso restringido al personal de apoyo tercerizado, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este sea requerido. Este acceso debe ser autorizado y monitoreado.
- Se deberían revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

Para la seguridad física de las oficinas se deberían considerar las siguientes pautas:

- Se debería tomar en cuenta regulaciones y estándares de salud y seguridad.
- Se deben instalar equipos con clave para evitar el acceso del público.
- Donde sea aplicable, los edificios deben ser discretos y deben dar una mínima indicación de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información.
- Los directorios y las guías telefónicas internas identificando locaciones de los recursos de información sensible no deben ser fácilmente accesibles por el público.

## Guía de implementación de la cláusula de Gestión de comunicaciones y operaciones (GC)

Para proteger la documentación de sistemas de accesos no autorizados se debería considerar las siguientes pautas:

- La documentación de sistemas se debería almacenar con seguridad.
- La lista de acceso a la documentación se sistemas se debería limitar al máximo, y ser autorizada por el propietario de la aplicación.
- La documentación de sistemas mantenida en una red pública o suministrada vía una red pública, se debería proteger adecuadamente.

Por otro lado, los registros de auditoría deberían incluir, cuando sea relevante:

- Identificaciones de usuarios.
- Fecha y hora de conexión y desconexión.
- Identidad del terminal o locación si es posible.
- Registros de éxito y fracaso de los intentos de acceso al sistema.
- Registros de éxito o fracaso de datos y de otros intentos de acceso a recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de las instalaciones y aplicaciones del sistema.
- Archivos accedidos y el tipo de acceso.
- Direcciones de red y protocolo.
- Las alarmas realizadas por el sistema de control de accesos.
- Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos.

El nivel de monitoreo requerido para las instalaciones individuales debe ser determinado por una evaluación de riesgos. Una organización debe cumplir con todos los requerimientos legales aplicables a sus actividades de monitoreo. Las áreas que deben ser consideradas incluyen:

- Acceso autorizado, incluyendo detalles como:
  - ✓ La identificación del usuario.
  - ✓ La fecha y hora de los eventos clave.
  - ✓ El tipo de evento.

  - ✓ Los archivos ingresados.
  - ✓ El programa o recursos utilizados.
- Todas las operaciones privilegiadas como:
  - ✓ Uso de cuentas privilegiadas, como supervisores, administradores.
  - ✓ Puesta en marcha y parada del sistema.
  - ✓ Conexión o desconexión de un recurso de entrada o salida.
- Intentos de accesos no autorizados, como:
  - ✓ Intentos fallidos.
  - ✓ Acciones con fallas o rechazadas que involucran datos y otros recursos.
  - ✓ Violaciones a la política de acceso y las notificaciones de los firewalls y entradas de red.
  - ✓ Las alertas de los sistemas de detección de intrusos del propietario.
- Alertas o fallas del sistema, como:
  - ✓ Alertas o mensajes de consola.
  - ✓ Excepciones de registro en el sistema.
  - ✓ Alarmas de la gerencia de red.
  - ✓ Alarmas levantadas por los sistemas de control de accesos.
- Cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad.

## Guía de implementación de la cláusula de Control de accesos (CA)

Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. Los controles de acceso son lógicos y físicos y estos deben ser considerados juntos. Se debería dar a los usuarios y proveedores de servicios una especificación clara de los requisitos de negocio cubiertos por los controles de acceso.

Esta política debería contemplar lo siguiente:

- Requisitos de seguridad de cada aplicación de negocio individualmente.
- Identificación de toda la información relativa a las aplicaciones y los riesgos que la información está enfrentando.
- Políticas para la distribución de la información y las autorizaciones.
- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes.
- Legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios.
- Perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajo.
- Administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión.
- Segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos.

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro, que debería incluir:

- La utilización de un identificados único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarse de sus acciones.
- La comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información.
- Verificación de la adecuación del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad de la organización.
- La entrega a los usuarios de una relación escrita de sus derechos de acceso.

- La petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso.
- La garantía de que no se provea acceso al servicio hasta que se haya completado los proceso de autorización.
- El mantenimiento de un registro formalizado de todos los autorizados para usar el servicio.
- La eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella.
- La revisión periódica y eliminación de identificadores y cuentas de usuarios redundantes.

Se debería controlar la asignación de privilegios, por un proceso formal de autorización en los sistemas multiusuario. Se deberían considerar los pasos siguientes:

- Identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación.
- Asignar privilegios a los individuos según los principios de “necesidad de sus uso” y “caso por caso” y en línea con la política de control de acceso.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios.

El proceso de controlar la asignación de contraseñas debe incluir los siguientes requisitos:

- Requerir que los usuarios firmen un compromiso para mantener secreto sus contraseñas personales y las compartidas por un grupo solo entre los miembros de dicho grupo.
- Proporcionar inicialmente una contraseña temporal segura que forzosamente deben cambiar inmediatamente después.
- Establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de reemplazo o temporal.

- Establecer un conducto seguro para hacer llegar las contraseñas temporales a los usuarios. Se debería evitar su envío por terceros o por mensajes no cifrados de correo electrónico.
- Las contraseñas temporales deben ser únicas para cada individuo y no deben ser obvias.
- Los usuarios deberían remitir acuse de recibo de sus contraseñas.

## Guía de implementación de la cláusula de Adquisición, desarrollo y mantenimiento de sistemas de información (ADM)

Para minimizar la corrupción de los sistemas de información, se deberían mantener estrictos controles sobre la implantación de cambios. La introducción de nuevos sistemas y cambios mayores al sistema existente debe seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación.

Este proceso debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios. Este proceso debe también asegurar que no se comprometa la seguridad y los procedimientos de control existentes, que a los programadores de soporte se les dé acceso solo a partes del sistema necesarias para su trabajo y que se debe tener una aprobación y acuerdo formal para cualquier cambio.

La aplicación y sus procedimientos de control de cambios deberían estar integrados siempre que sea posible. Este proceso debería incluir:

- El mantenimiento de un registro de los niveles de autorización acordados.
- La garantía de que los cambios se realizan por usuarios autorizados.
- La revisión de los controles y procedimientos de integridad para asegurarse que los cambios no los debilitan.
- La identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora.
- La obtención de la aprobación formal para propuestas detalladas antes de empezar el trabajo.
- La garantía de la aceptación por parte del usuario autorizado de los cambios antes de cualquier implantación.

Además se deberían revisar y probar las aplicaciones cuando se efectúen cambios. Este proceso debería incluir:

- La revisión de los procedimientos de control de la aplicación y de la integridad para asegurar que los cambios en el sistema operativo no han sido comprometidos.
- La garantía de que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema que requieran los cambios del sistema operativo.

- La garantía de que la modificación de los cambios del sistema operativo se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación.

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Anexo 7:

# Políticas Planteadas

**Hans Ryan Espinoza Aguinaga**

**20047270**

**ASESOR: Dr. Manuel Tupia Anticona.**

# Política de Asignación de equipos de cómputo, telefonía y celulares

## I. Objetivo:

Regular la administración de la asignación de equipos de cómputo, telefonía y celulares a personal de la empresa.

## II. Alcance:

Esta política contempla a todos los equipos de cómputo, telefonía y celulares que el área de Sistemas tiene a su cargo y que pueda ser asignado permanente o temporalmente a personal de la empresa, incluyendo a empleados, practicantes y personal de outsourcing. Esta política establece los lineamientos acerca de la solicitud, aprobación, asignación o reasignación, y desincorporación por obsolescencia de los equipos de cómputo y celulares.

## III. Definiciones:

- Equipos de cómputo y telefonía: Cualquier dispositivo que el área de Sistemas administra y suministra al personal que lo requiera, tales como: PCs, laptops, impresoras, teléfonos fijos, entre otros.

- Celulares: Equipos celulares contratados a operadores de telefonía local que el área de Sistemas administra y suministra al personal que lo requiera.

## IV. Política:

A continuación se detalla la descripción de la presente política.

- Es responsabilidad de la Gerencia de Sistemas evaluar las alternativas tecnológicas existentes en el mercado con la finalidad de proveer equipos de computación acordes con los requerimientos de la Empresa.
- La Gerencia de Sistemas deberá elaborar anualmente los planes de adquisición de equipos de cómputo y celulares que requiera la Compañía tomando como base los estándares aprobados y lo establecido en la política de activos fijos de la empresa.
- Toda solicitud de equipos de cómputo y celulares deberá ser realizada por la Gerencia del usuario solicitante a través del responsable designado por la

Gerencia de Sistemas, previa aprobación del Director o Gerente del área correspondiente y de la Gerencia de Sistemas, con los tiempos de anticipación establecidos. Dicha aprobación deberá contar con el sustento del requerimiento de acuerdo con las funciones y puesto del usuario solicitante.

- Es responsabilidad del área de compras evaluar los posibles proveedores y realizar las compras de los equipos recomendados por la Gerencia de Sistemas de Información o Tecnología de Información para satisfacer los requerimientos de la Empresa de acuerdo a lo establecido en la política de Compras del Área Andina y sobre la base de los acuerdos corporativos establecidos.
- En aquellos casos donde el activo a adquirir no se comercialice en el país y localidad solicitante y el tiempo de entrega pueda exceder lo contemplado inicialmente, la Gerencia de Sistemas deberá notificar al usuario solicitante la fecha estimada de entrega del equipo solicitado.
- La asignación, reasignación, administración, distribución y mantenimiento de los equipos de cómputo es responsabilidad de la Gerencia de Sistemas. Para el caso de los mantenimientos y gestiones referidas al cumplimiento de garantías, la Gerencia de Sistemas deberá canalizarlo a través de los proveedores correspondientes.
- Todos los movimientos de equipos de cómputo serán efectuados por la Gerencia de Sistemas previa solicitud del área que lo requiera y deberán ser notificados inmediatamente a la Gerencia o Coordinación de Contabilidad para su incorporación o actualización en el sistema contable respectivo.
- La Gerencia de Sistemas deberá evaluar y proveer a los usuarios, los equipos que satisfagan la carga de trabajo requerida y las ventajas técnicas adicionales de acuerdo a su función y puesto.
- Toda solicitud de equipos que no se encuentren definidos bajo los estándares de la compañía, no cumplan con la normativa establecida en esta política y puedan ser catalogados como riesgosos para la Compañía, deberán ser autorizados por la Gerencia de Sistemas.
- Será responsabilidad de la Gerencia de Sistemas atender todas las solicitudes y reclamos a través del Service Desk o Soporte de Comunicaciones, según sea el caso.

V. Disposiciones particulares:

- Auditoría y Revisión

  La Gerencia de Sistemas será la responsable de realizar revisiones periódicas (cada 6 meses) de la presente política a fin de revisar si existe algún cambio relevante que deba ser indicado en el presente documento.

- Excepciones

  Las excepciones a esta política deberán ser aprobadas por la Gerencia de Sistemas de la empresa o la persona que él designe.

- Sanciones

  Las acciones que incumplan al presente procedimiento se harán efectivas de acuerdo con la falta cometida y a la evaluación realizada por las Gerencias competentes.

# Política para el desarrollo de aplicaciones

## I. Objetivo:

Contemplar aspectos de seguridad de información a ser incluidos dentro de los sistemas de información aplicando mejores prácticas y lineamientos en el desarrollo de aplicaciones.

## II. Alcance:

Este lineamiento incluye textos de la norma ISO/IEC 17799 (2002 y 2005) y de la metodología de desarrollo de aplicaciones en la plataforma Microsoft, a fin de considerarlos como mejores prácticas en seguridad de la información a ser incluidos en los sistemas de información desarrollados y utilizados en la Compañía. Este lineamiento contempla la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios.

## III. Lineamientos Generales:

A continuación se detalla la descripción del presente lineamiento referente al proceso de desarrollo de sistemas.

- Indicar explícitamente en los requerimientos del negocio para sistemas nuevos o mejoras a sistemas existentes *los controles de aplicación* que van a ser implementados en el desarrollo de las mismas. Dichas especificaciones deberían considerar los controles automatizados a ser incorporados en el sistema y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares cuando se evalúen paquetes de software para aplicaciones de negocio.
- Validar los datos de entrada a las aplicaciones del sistema para garantizar que estos sean ingresados de manera correcta y apropiada. Se deberían aplicar verificaciones *a la entrada de las transacciones*, *de los datos de referencia* (por ejemplo nombres y direcciones, límites de crédito, números de clientes) *y de las tablas de parámetros* (por ejemplo precios de venta, tasas de cambio de monedas, tasas de impuestos, entre otros).
- Verificar que los datos ingresados al sistema no hayan sido corrompidos por errores del proceso o por actos deliberados. Se deberían incorporar a los sistemas, comprobaciones de validación para detectar dicha corrupción. El

diseño de las aplicaciones debería asegurar la implantación de controles que minimicen el riesgo de los fallos del proceso con pérdidas de integridad.

- Los controles requeridos dependerán del diseño de la aplicación y de la complejidad de la corrupción de los datos que puedan impactar en el negocio.
- Validar los datos de salida de los sistemas de información para garantizar que el proceso de la información ha sido correcto y ha culminado satisfactoriamente a través de controles de aplicación. Dichos controles incluirán la validación, verificación y prueba de los datos.
- Los controles criptográficos se podrían determinar previamente, desde el diseño del sistema como posteriormente, luego de la evaluación de riesgos. Dependiendo del momento en que se definan dichos controles, se podrá especificar si las medidas criptográficas son aplicables al sistema de información y se podrá definir qué tipo de control criptográfico se debería aplicar, con qué propósito y en qué procesos del negocio.
- Para asegurar que cualquier modificación de los archivos, librerías o cualquier objeto de los programas fuentes sean manejados a cabo de una forma segura, se deberían tomar en cuenta los siguientes controles: *Control del software en producción, protección de los datos de prueba del sistema, control de acceso a las librerías de programas fuente.*
- Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.
- No se recomiendan modificaciones a los paquetes de software. Se deberían usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea factible.
- Considerar los siguientes controles a fin de mitigar posible código malicioso o encubierto en los sistemas de información o software:
    - Adquirir programas solamente de fuente confiable;
    - Adquirir programas en código fuente de tal forma que el código pueda ser verificado
    - Utilizar productos evaluados
    - Inspeccionar todo código fuente antes de su uso operativo
    - Controlar el acceso y las modificaciones en todo código una vez implementado

- Utilizar personal de confianza para trabajar en los sistemas clave del negocio

- Se deberían considerar los siguientes controles cuando se tercerice el desarrollo de software:
    - Acuerdos bajo licencia, acuerdos de confidencialidad de información, propiedad del código y derechos de propiedad intelectual.
    - Certificación de la calidad y exactitud del trabajo realizado.
    - Acuerdos acerca de fallas posteriores a la implementación.
    - Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
    - Requisitos contractuales sobre la calidad del código.
    - Pruebas antes de la implantación para detectar posible código malicioso o encubierto.

VI. Disposiciones particulares:

- Auditoría y Revisión

  La Gerencia de Sistemas será la responsable de realizar revisiones periódicas (cada 6 meses) de la presente política a fin de revisar si existe algún cambio relevante que deba ser indicado en el presente documento.

- Excepciones

  Las excepciones a esta política deberán ser aprobadas por la Gerencia de Sistemas de la empresa o la persona que él designe.

- Sanciones

  Las acciones que incumplan al presente procedimiento se harán efectivas de acuerdo con la falta cometida y a la evaluación realizada por las Gerencias competentes.

# Política para los cambios a sistemas de aplicación

## I. Objetivo:

El objetivo de la presente política es definir los lineamientos a seguir en el proceso de Change Management para todas las modificaciones (incidentes o mejoras) para aplicaciones locales pertenecientes a la plataforma Windows, como así también los requisitos mínimos que deben cumplir los proyectos de implementación o cambio de versión de sistemas aplicativos locales.

## II. Alcance:

Se encuentran alcanzadas por la presente política todas las aplicaciones de la plataforma Windows que cumplan con alguna de las siguientes características:

a. Aplicaciones desarrolladas por el equipo de Soporte local.
b. Aplicaciones desarrolladas por consultoras externas, pero cuyo código fuente sea propiedad de la empresa.
c. Aplicaciones de terceros sujetas a cambios realizados por el equipo de Soporte. En este caso solo se mantendrán los objetos a ser modificados.

Asimismo, se encuentran alcanzados todos los proyectos de implementación o cambio de versión de sistemas aplicativos locales.

## III. Lineamientos Generales:

1) Procedimiento de manejo de Códigos Fuente

- Se deben mantener en línea las últimas dos versiones del código fuente u objetos a ser modificados.
- La administración del código fuente de las aplicaciones u objetos a ser modificados es realizada únicamente por parte de los Managers y Project Managers del área de sistemas.
- Dentro del directorio debe existir un directorio con el nombre de la aplicación a resguardar y una subcarpeta con cada versión de la misma.
- Cada actualización de códigos fuentes debe ir acompañada por un archivo log indicando las modificaciones realizadas a dicho código fuente.

- En el caso de requerirse por parte de un programador o consultor externo, la última versión del código fuente de una aplicación, se deberá solicitar el mismo al Project Manager responsable del control de la aplicación a ser modificada. Tanto la solicitud de códigos fuentes como la entrega de nuevas versiones de códigos fuentes deben quedar registradas en un mail.

2) Procedimiento de Change Manegement – aprobación sobre cambios a los aplicativos, puesta en producción y test.
    - El procedimiento de Change Manangement será administrado a través de la aplicación ClearQuest.
    - En ClearQuest deberá existir un Group dentro del Systemgroup de Sistemas de Cono Sur para cada una de las aplicaciones alcanzadas por el procedimiento de Change Management. De requerirse, se podrá separar los Grupos por módulos de la aplicación.
    - En el caso de tratarse de aplicaciones de terceros, todo cambio en las mismas deberá ser informado previamente a sistemas, creándose un CR que respalde cualquier tipo de modificación. En el caso de existir cambios no informados por el usuario o el proveedor, se informará a los responsables de las áreas involucradas a los efectos de tomar las acciones correctivas necesarias.

# Política de protección de la información propietaria y de escritorio limpio

## I. Objetivo:

Esta política tiene por objeto establecer pautas y lineamientos de conducta afectados a la protección, guarda y conservación segura de la documentación y/o información sensitiva y confidencial del negocio. Es objeto de ésta política, alentar a todos los empleados a modificar sus hábitos de conducta, en virtud de asegurar la confidencialidad de la documentación propietaria y de toda documentación compañía que por determinada razón, accedan o posean en forma circunstancial.

Se define Información Propietaria como cualquier información que incluya datos sensibles y confidenciales sobre los empleados y las operaciones de la empresa. Algunos ejemplos son: Informes financieros, fórmulas, documentos legales, investigación de mercado. Las direcciones de e-mail, números de teléfono del lugar de trabajo, y los particulares del personal y las planillas de sueldos son también considerados Información Propietaria.

## II. Alcance:

Las pautas y lineamientos establecidos en esta norma, son de aplicación y cumplimiento asociado a TODAS las tareas, funciones y responsabilidades de TODOS los empleados de la empresa.

## III. Pautas de custodia y resguardo de información y documentación:

Los siguientes principios proporcionan una guía para asegurar que nuestro ámbito de trabajo, se transforme en un lugar seguro y afectado al resguardo de la documentación y/o información sensitiva y confidencial, asociada con las actividades de negocios de la empresa.

Deberá Ud. ser consciente de la información y prácticas de negocios que puedan dar a un competidor ventajas sobre usted o la Compañía.

- Siempre sepa con quién se está comunicando. Verifique la identidad de cualquiera que diga que es de una compañía que trabaja con la empresa.

- Obtenga el nombre de la persona, empresa, número telefónico y su número de documento y llame a la Compañía para verificar que la persona sea un empleado.
- No revele información personal o de negocios sin antes saber cómo será utilizada.
- No incluya información sensible del negocio en e-mail (a menos que utilice un encriptado aprobado).
- Nunca discuta información sensible de la Compañía por teléfono.
- Nunca hable de información sensible del negocio en lugares públicos.
- No discuta información sensible con personas ajenas a la Compañía, a menos que tenga una "necesidad de saber".
- Deshágase de información de la Compañía siguiendo las políticas de manejo de documentación de la Compañía, retención y eliminación.

*Oficinas Privadas:*

- Los empleados que ocupan una oficina total o parcialmente cerrada, deberán resguardar documentación e información propietaria / activos, en mobiliarios, cajas de seguridad (cuando se trate de valores, certificaciones de propiedad u otra documentación similar) o cajoneras personales, con cerraduras de seguridad con llave.
- Será responsabilidad de los empleados ocupantes de oficinas, contemplar los riesgos inherentes a la seguridad de la información sensible en su poder, solicitando al responsable del sector de Servicio de Oficina, todos los elementos necesarios para asegurar la guarda y conservación de los mismos.
- En todos los casos, el empleado deberá contemplar el estado de seguridad de la documentación y de los bienes asignados en sus momentos de ausencia, limitando el posible acceso a su oficina y/o practicando su guarda bajo llave.
- Los empleados poseedores de oficinas, serán únicos responsables por la pérdida, extravío o destrucción de la documentación y/o de los bienes asignados, siempre que no se verifique una violación expresa al recinto y/o a los instrumentos elegidos para guarda y conservación.

- Los empleados que ocupan oficinas privadas no podrán limitar el acceso a las mismas al finalizar su jornada laboral o durante períodos prolongados de ausencia, permitiendo el aseo y mantenimiento del recinto. Esta acción, no limita su responsabilidad y deberá contemplar, según se establece en los puntos anteriores, la correcta guarda y conservación de los elementos y de la información sensible del negocio.

*Espacios de trabajo abiertos:*

- Los empleados que trabajen en espacios abiertos (ubicaciones de piso de administración) deberán contemplar los riesgos inherentes a la seguridad de la información sensible en su poder, y solicitar al responsable del sector de Servicio de Oficina, todos los elementos necesarios para asegurar la guarda y conservación de los mismos.
- Con el objeto de minimizar riesgos, los empleados que trabajen en espacios abiertos, deberán asegurarse que el mobiliario asignado (cajones, muebles, etc.) posea la capacidad adecuada a los efectos de archivo sectorial, con cerradura y llave por duplicado.
- Los empleados deberán identificar las llaves y entregarán copia de éstas al responsable del área o sector al que pertenecen, a los efectos de permitir el acceso a la documentación a dicho responsable, en caso de ausencia del empleado y bajo necesidad de urgencia.
- Cuando la documentación supere en volumen de capacidad al mobiliario asignado, dicha documentación deberá ser clasificada y claramente identificada, para ser remitida al Archivo General de la Organización.

IV. Disposiciones generales:

La política de Protección de la Información Propietaria (POPI) y de Escritorio Limpio requiere a TODOS los empleados que:

- Protejan la información sensible del negocio como por ejemplo, toda información de planeamiento comercial o financiero y documentos contables, análisis de investigación de mercado, desarrollo de nuevos producto, planes de fabricación y producción, estrategias de venta, información del personal, información del cliente y/o consumidor, etc.; del robo o acceso / uso no autorizados.

- Aseguren la información sensible cuando no se encuentran en su espacio laboral luego del horario de trabajo, cuando estén de viaje de negocios / feriados / vacaciones o, cuando utilizan impresoras, fotocopiadoras o equipos de fax comunitarios.
- Resguarden todos los elementos y documentos sensibles de negocios, disquetes de computadora, discos compactos y equipos de computación portátiles tales como computadoras laptop, PDA´s, equipos inalámbricos de correo electrónico, teléfonos celulares, videos y otros, utilizando:

  - ✓ Un compartimento bajo llave, como un cajón de escritorio o un gabinete.
  - ✓ Cerraduras para asegurar dentro de los límites de oficinas, que la misma permanezca cerrada durante los períodos de ausencia, siempre que algún responsable del sector conserve copia de la llave de ingreso para asegurar aseo y mantenimiento del recinto.
  - ✓ Elementos, que en el caso de las computadoras portátiles, se pueden asegurar a su terminal con un seguro / cable especial, diseñado para este propósito; las computadoras personales, deben ser apagadas al final de cada día laboral.
  - ✓ Contraseñas seguras y acceso restringido a las computadoras personales, las cuales deben apagarse al finalizar la jornada laboral y las contraseñas deben ser protegidas en forma adecuada, no deben ser escritas y ocultas en lugares predecibles o pegadas en un papel debajo del escritorio, etc.
  - ✓ Protectores de pantalla activos durante la jornada laboral, cuando los empleados están ausentes de sus oficinas o fuera del área de trabajo inmediato, con contraseñas que se activan automáticamente después de transcurrido un período designado de inactividad.

Los empleados notificaran al responsable del sector de Servicio de Oficina, de todos los elementos de seguridad faltantes o en condiciones de reparación, necesarios para asegurar la guarda y conservación de los mismos, e informarán a la gerencia del área o sector del pedido realizado, al momento de efectuarse el mismo.

## Política de administración de usuarios privilegiados

I. Objetivo:

Regular la definición y la administración de los usuarios administradores de los sistemas operativos y software de base (usuarios privilegiados).

II. Alcance:

Esta política contempla a todos los usuarios administradores existentes en los sistemas operativos y software de base como recursos esenciales para la instalación y administración de dichos sistemas (Administradores en Servidores Windows 2000, Administradores de Bases de datos, Administradores en los equipos de comunicación, entre otros).

III. Definiciones:

- *Sobre lacrado:* sobre de papel, el cual es cerrado de manera que se pueda evidenciar la violación del mismo, a través de alguna ruptura u otro mecanismo que asegure que la información contenida dentro del mismo ha sido comprometida. Dentro del sobre lacrado se colocarán las contraseñas de los usuarios privilegiados. Dicho sobre deberá mostrar exteriormente la fecha del lacrado, así como el nombre de la persona que lo lacró.

IV. Política:

A continuación se detalla la descripción de la presente política.

- De ser técnicamente posible, todos los usuarios que por defecto incorporen los sistemas operativos y software de base deberán ser renombrados o inhabilitados y reemplazados por otros, contando con los mismos atributos, pero con nombres y contraseñas diferentes, a fin de que en caso de intentos de penetración a la seguridad establecida, no resulte obvio el nombre de los mismos. Todos los usuarios privilegiados existentes deberán ser debidamente documentados por el Líder de Proyectos de Tecnología.
- Los nombres que se generen deberán respetar un estándar definido por el Líder de Proyectos de Tecnología (según los estándares corporativos), y deben pasar por desapercibidos frente a los demás usuarios.
- No debe existir en las plataformas más de un usuario con estas características. Las excepciones deberán ser justificadas técnica y

funcionalmente por el máximo responsable de la plataforma tecnológica, y deberán ser autorizadas por el Líder de Proyectos.

- Estos usuarios no deberán ser utilizados para tareas de administración de la seguridad y su actividad deberá ser auditada mediante la revisión de los registros en los logs correspondientes.
- Los usuarios privilegiados solo deberán ser utilizados para las circunstancias estrictamente necesarias como son la instalación de software, procesos o actividades de administración que no puedan ser llevados a cabo por usuarios de menor acceso o menores privilegios. Las cuentas de los usuarios privilegiados (“Administrador”, “root”, “sa”) deben ser utilizadas, salvo en casos de emergencia o incidentes, quedando debidamente documentados en la Bitácora de utilización especial de contraseñas de usuarios privilegiados.
- Es de responsabilidad directa del Líder de Proyectos de Tecnología, el conocimiento de las contraseñas de los usuarios privilegiados. El será el responsable de controlar su conocimiento, y de existir algún indicio en el compromiso de las contraseñas, será el responsable de cambiarlas inmediatamente.
- Las contraseñas de los usuarios privilegiados deberán ser guardadas en un sobre lacrado en custodia del Gerente de Sistemas bajo llave. Una copia del mismo, deberá ser custodiada por el Responsable de Security&Controls. En caso surja algún incidente en el cual no se encuentre el Líder de Proyectos de Tecnología y se necesite de las contraseñas de acceso de los usuarios privilegiados, el Gerente de Sistemas deberá abrir el sobre lacrado. Cualquier incidente que requiera romper las contraseñas contenidas en el sobre lacrado deberán ser registradas en la Bitácora de utilización especial de contraseñas de usuarios privilegiados.
- En caso el Gerente de Sistemas ni el Líder de Proyectos de Tecnología se encuentren y sea necesario romper las contraseñas, el Líder de Proyectos de Security&Controls será el responsable de abrir el sobre lacrado y utilizar las contraseñas necesarias.
- En caso el sobre lacrado se abra por alguna emergencia o incidente, el Líder de Proyectos de Tecnología deberá cambiar las contraseñas utilizadas, destruir los sobres lacrados existentes y deberá guardar las nuevas contraseñas en sobres lacrados nuevos. Dicho sobre deberá ser

custodiado por el Gerente de Sistemas bajo llave y una copia del mismo deberá ser custodiado por el Responsable de Security&Controls.

V. Disposiciones particulares:

- Auditoría y Revisión

  El Responsable de Security & Controls será responsable de realizar revisiones periódicas (**cada 6 meses**) de los sobres lacrados, para lo cual el Gerente de Sistemas firmará su revisión en el formato de revisión.

- Excepciones

  Las excepciones a esta política deberán ser aprobadas por la Gerencia de Sistemas de la empresa o la persona que él designe.

- Sanciones

  Las acciones que incumplan al presente procedimiento se harán efectivas de acuerdo con la falta cometida y a la evaluación realizada por las Gerencias competentes.

# Política de retención de documentos

## I. Objetivo:

Establecer los lineamientos que regirán el proceso de retención de los documentos que se generan en las diferentes áreas de la Compañía a fin de asegurar la integridad de la información que soporta las operaciones contables, financieras, legales y administrativas y cumplir con las leyes y reglamentos que regulan la retención de los documentos.

## II. Alcance:

Esta política es aplicable a todas las unidades de negocio, responsables de la custodia de los documentos contables, financieros, legales y administrativos que se deriven de las operaciones de la Compañía.

## III. Definiciones:

- *Documentos contables:* Se refiere a los Libros originales de entradas contables que incluyen, Libros de Ventas, el balance general y los balances subsidiarios, los registros de facturas relacionados y los archivos informales y memorandos como hojas de trabajo que apoyen asignaciones de costos, confirmaciones y conciliaciones, facturas o recibos que soporten los gastos, inversiones, cumplimiento de obligaciones tributarias, parafiscales, entre otras de fuente legal.
- *Documentos financieros:* Se refiere al material documental de corroboración o soporte de registros de índole financiero que incluye, entre otros, cheques, facturas, contratos, actas de reuniones, confirmaciones y otras representaciones escritas.
- *Documentos legales:* Se refiere al material documental relacionado con aspectos legales de la Compañía, tales como: Libros Corporativos: Actas de Junta Directiva, Asambleas de Accionistas y Libro de Acciones, contratos, acuerdos, convenios, archivos de arbitraje y negociaciones internacionales, opiniones legales, entre otros.
- *Documentos administrativos:* Se contemplan en ésta categoría aquellos documentos de carácter administrativo, los cuales no generan operaciones o registros contables, sin embargo representan valor para la Compañía, dado que soportan sus operaciones regulares. Entre ellos encontramos: las

políticas, manuales de procedimientos, solicitudes de empleo, registro de proveedores, estudios de mercado, actividades de mercadeo, actividades promocionales, archivos de personal, cumplimiento de obligaciones laborales, correspondencia, entre otros.

IV. Lineamientos Generales:

- Las unidades organizativas responsables de la custodia de los documentos contables, financieros, legales y administrativos de la Compañía, serán responsables del estricto cumplimiento de esta política.
- La retención de los documentos en las diferentes unidades organizativas se realizará de acuerdo al período de tiempo establecido en los anexos a este documento
- Las declaraciones de impuestos, recibos y Estados Financieros serán retenidos por la Gerencia de Finanzas o unidades responsables de su emisión permanentemente, como el Departamento de Contabilidad, Cuentas por pagar, Recursos Humanos y relacionados.
- Las unidades organizativas responsables de la custodia de los documentos contables, financieros, legales y administrativos, deberán mantenerlos archivados durante el tiempo establecido para su retención, en un lugar seguro y en condiciones idóneas que garanticen su integridad, conservación y disponibilidad para su consulta. No deberán ser rayados ni mutilados.
- Las unidades organizativas responsables de la custodia de los documentos contables, financieros, legales y administrativos, serán responsables de efectuar revisiones periódicas de sus archivos, a fin de desincorporar los documentos que hayan cumplido con el período de retención establecido en esta política.

V. Disposiciones particulares:

- Auditoría y Revisión

  La Gerencia de Sistemas será la responsable de realizar revisiones periódicas (cada 6 meses) de la presente política a fin de revisar si existe algún cambio relevante que deba ser indicado en el presente documento.

- Excepciones

Las excepciones a esta política deberán ser aprobadas por la Gerencia de Sistemas de la empresa o la persona que él designe.

- Sanciones

  Las acciones que incumplan al presente procedimiento se harán efectivas de acuerdo con la falta cometida y a la evaluación realizada por las Gerencias competentes.