Este es un plan de seguridad desarrollado para la empresa Kohtech, el cual explicaremos todas las amenazas y vulnerabilidades que puede tener la empresa al ser expuesta a los distintos ataques informáticos, problemas del día a día o catástrofes naturales.



****

**Plan de seguridad - Madrid**

| **Ataque/**  **Amenaza** | **Categoría/**  **Tipo** | **Daño** | **Riesgo/**  **Probabilidad** | **Medida de seguridad** | **Categoría** |
| --- | --- | --- | --- | --- | --- |
| Incendio | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Explosión de gas | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Terremoto | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Inundación | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Volcán | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Fallo eléctrico | Interrupción.  Físico | Pérdida de unos minutos de trabajo,ya que tarda poco en volver la luz. | (baja) | Backup  externo,información en la nube. | Restauración |
| Tormenta de nieve | Interrupción. Físico | Posible pérdida de electricidad, inundación posterior e imposibilidad de acceso. | (baja) | Backup  externo,información en la nube. | Restauración |
| Huracán | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Tornado | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Rayo | Interrupción. Físico | Pérdida de unos minutos de la información porque puede llegar a dejar sin luz a la empresa. | (muy baja) | Trabajar online y que se guarde automático. | Restauración |
| Tsunami | Interrupción Físico | Pérdida de toda la información en los dispositivos de la empresa. | (nula) | Nada. | Prevención |
| Se abre una falla en el suelo y hunde la calle de la sede | Interrupción  Físico | Pérdida total de la información y del material de trabajo. | (muy baja) | Información en la nube. | Prevención |
| Tormenta de arena | Interrupción Físico | Pérdida de poca información,posible pérdida de ordenadores físicos. | (muy baja) | Información en la nube. | Prevención |
| Cae un árbol en la puerta de la empresa que impide el acceso al edificio | Interrupción. Físico | Imposibilita el acceso de los trabajadores a la empresa, lo que puede derivar en imposibilidad de solventar errores. | (muy baja) | Tener una puerta adicional en otro lado del edificio. Posibilidad de trabajo en remoto. | Prevención |
| Meteorito cae en la sede | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| Disturbios violentos | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| Derrumbamiento | Interrupción Física | Pérdida de toda la información en los dispositivos de la empresa. | (baja) | Backup externo, información en la nube. | Prevención o Restauración |
| Corrupción de documentos debido al uso de licencias pirata | Interrupción | Pérdida de información además de que aumenta la posibilidad de sufrir ataques. | (baja) | Uso de productos con licencias oficiales. | Prevención |
| Virus | Malware.Lógica | Detección de sistema, borrado de archivos y comportamientos erróneos. | (baja) | Antivirus, cortafuegos, copias de seguridad, análisis del sistema. | Prevención |
| Gusano | Malware. Lógica | Explotar errores de configuración de la red  bien explotar agujeros de seguridad en el sistema operativo y las aplicaciones. | (baja) | Análisis de programas,antivirus, software anti malware. | Prevención |
| Adware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (baja) | App lock. | Interrupción |
| Spyware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (baja) | Leer antes de aceptar las condiciones de páginas, tener actualizado el software. | Prevención |
| Keylogger | Malware. Lógica | Descifrar contraseñas y otra información ingresada con el teclado. | (baja) | Antivirus,copias de seguridad. | Prevención |
| Troyano | Malware. Lógica | Violaciones de privacidad, cómo usar la webcam, borrar el disco... | (baja) | Antivirus y análisis de dispositivos de entrada en el ordenador. | Prevención |
| Hijackers | Malware. Lógica | Modificación la redirección de los servidores DNS. | (baja) | Prestar especial atención a todo lo que instalamos en nuestro ordenador y qué sitios de internet estamos visitando. y servicios de hosting en los que podemos registrar un dominio seguro. | Prevención |
| Crackers | Malware. Lógica | Copia, rono, manipulación o eliminación de datos. | (media/baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Hackers | Malware. Lógica | Realizar muchos de los demás ataques nombrados como la activación de un virus, robo de información importante y modificación de las contraseñas establecidas. | (media) | Software, contraseñas distintas. | Prevención y modificación |
| Pharming | Malware. Lógica | Engaña a las víctimas para que entreguen credenciales de todo tipo de cuentas confidenciales, tales como correo electrónico, intranets corporativas y mucho más. | (baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Cookies | Malware. Lógica | No pueden infectar ordenadores con virus ni otro tipo de malware, pero algunos ciberataques secuestran las cookies y, por lo tanto, las sesiones de navegación. El peligro está en su capacidad de hacer un seguimiento de los historiales de navegación de las personas. | (muy alta) | App lock. | Prevención |
| Spam | Malware. Lógica | Puede causar daños significativos, infectando las computadoras de los usuarios con software malicioso capaz de dañar los sistemas y robar información personal. También puede consumir recursos de la red. | (muy alta) | No propagues los correos tipo ‘cadena’, utiliza la opción CCO, borra el encabezamiento**...** | Prevención |
| Hoaxes | Malware. Lógica | La pérdida de productividad, pérdida de credibilidad, saturación de redes locales y de mensajes. | (alta) | Estar atentos a temporales, faltas de ortografía y cadenas, usan imágenes de google... | Prevención y actuar de raiz |
| Doxing | Malware. Lógica | Conseguir información de la persona para así presionarla. No es un ataque en sí, consiste en recopilar información de las páginas web de las que el usuario entra. | (media) | No usar demasiadas redes sociales o evitar dar datos personales | Prevención |
| Phishing | Malware. Lógica | Manipular a la persona para que le de contraseñas,es decir, suplantar la identidad de una empresa.O obtener datos bancarios | (alta) | Tener cuidado con los correos o con la información que se envía,verificar la web donde se acceda | Prevención |
| Ping Flood | Malware. Lógica | Ping flood se basa en enviar a la víctima una cantidad abrumadora de paquetes ping. | (baja) | Tener un buen sistema operativo. | Prevención |
| Ping de la muerte | Malware. Lógica | El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. | (muy baja) | Casi todos los sistemas operativos de hoy en día rechazan esos paquetes. | Prevención |
| Escaneo de puertos | Malware. Lógica | Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles.  Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad. | (alta) | No abrir más puertos de los necesarios.Usar herramientas para comprobar los puertos abiertos.Utilizar cortafuegos.Equipos siempre actualizados. | Prevención y detección |
| ARP Spoofing | Malware. Lógica | ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo. | (alta) | Protegerse mediante los protocolos para consultar la IP | Prevención y detección |
| ACK flood | Malware. Lógica | Esta es una técnica para enviar un paquete TCP / ACK al objetivo a menudo con una dirección IP falsificada. | (media) | Usar cortafuegos para impedir el ataque | Prevención y detección |
| Ataque FTP Bounce | Malware. Lógica | El atacante puede conectarse a los servidores FTP y tiener la intención de enviar archivos a otros usuarios / máquinas que usan el comando PORT. Para que el servidor FTP intente enviar el archivo a otras máquinas en un puerto específico y verifique que el puerto esté abierto. | (media) | Deshabilitar el FTP estándar.Usar una encriptación potente y funciones hash | Prevención y detección |
| Ataque Man-In-The-Middle | Malware. Lógica | Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, sino que también pueden dirigir toda la información dentro de los dispositivos. | (alta) | Usar extensiones de correo de Internet seguras / multipropósito, o S / MIME.  Certificados de autenticación | Prevención. |
| ICMP Tunneling | Malware. Lógica | El tunneling se usa a menudo para eludir los firewalls que no bloquean los paquetes ICMP, o para establecer un canal de comunicación cifrado y difícil de rastrear entre dos computadoras sin interacción directa de la red. | (media) | Permitir a los administradores usar mensajes ICMP libremente.  Permitir el paso del gran tamaño de ICMP. | Prevención. |
| Ataque LOKI | Malware. Lógica | Este programa es una prueba de concepto que funciona para demostrar que los datos se pueden transmitir de forma secreta a través de una red escondiéndolos en el tráfico que normalmente no contiene cargas útiles. Se centra en el robo de datos bancarios, billeteras de criptomonedas y contraseñas de los navegadores web. | (medio) | Evitar abrir archivos de correo,porque se envía por ahí y es fundamental tener todo el paquete de office actualizado | Prevención. |
| Ataque de secuencia TCP | Malware. Lógica | Predice el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión. | (bajo) | Ahora mismo ya se han diseñado un algoritmo para generar números de secuencia aleatorios y que los atacantes no te los puedan adivinar | Prevención y detección |
| CAM Table Overflow | Malware. Lógica | La tabla CAM de un conmutador contiene información de red, como las direcciones MAC disponibles en los puertos físicos del conmutador y los parámetros de VLAN asociados. Los desbordamientos de la tabla CAM ocurren cuando una entrada de direcciones MAC se inunda en la tabla y se alcanza el umbral de la tabla CAM. Esto hace que el conmutador actúe como un concentrador, inundando la red con tráfico fuera de todos los puertos. | (medio) | Para prevenir este tipo de ataque, cambiaremos el puerto a un puerto de acceso emitiendo acceso en modo de puerto de conmutación. Luego asignaremos la cantidad máxima de direcciones MAC en las que se almacenará la tabla CAM para esta interfaz. | Prevención |
| Inyección SQL | Malware. Lógica | Ayuda al hacker a ejecutar un código debido a la presencia de vulnerabilidad en la capa de la base de datos de la Aplicación. En consecuencia, el código obtendrá datos confidenciales o incluso comprometerá la aplicación en sí. | (alto) | Limpiar las peticiones de caracteres especiales en SQL. Delimitar los valores en las consultas .Utilizar las últimas tecnologías.Escaneos regulares (con Acunetix) | Prevención |
| Cross-Site Request | Malware. Lógica | La falsificación de solicitudes entre sitios es un tipo de exploit malicioso de un sitio web mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. | (alto) | Navegar con atención y precaución.  Revisar el terminal en busca de malware.Protección frente a CSRF por parte del operario de la página web | Prevención y detección |
| Web Defacement | Malware. Lógica | La desfiguración del sitio web es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. | (alto) | Limitar los complementos de tu página web. Limitar los niveles de acceso. Escanear el código fuente de tu sitio | Prevención y detección |
| Buffer Overflow | Malware. Lógica | Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. | (medio) | Deshabilitar los servicios innecesarios. Proteja sus sistemas Linux, ya sea con un servidor de seguridad o un sistema de prevención de intrusiones basado en host (IPS). | Prevención y detección |
| Root kit | Malware. Lógica | El objetivo del atacante es obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. | (medio) | Instalar un sistema de seguridad.  Evitar abrir correos electrónicos de procedencia dudosa.  Evitar descargar archivos de sitios web extraños | Prevención |
| Caída de internet | Interrupción. Físico | Pérdida de tiempo de servicio. | (media) | Contar con varios proveedores de servicio de acceso a internet. | Prevención |
| Filtración de datos | Intercepción  Lógica | Los datos de los clientes pueden verse comprometidos. | (baja) | Implementar diversas medidas físicas y lógicas para evitar el acceso no autorizado a los datos. | Prevención |
| Averías físicas de los ordenadores | Interrupción. Físico | Pérdida de información, puede afectar al funcionamiento/rendimiento de un equipo. | (media) | Contar con personal de mantenimiento eficaz y reparación. | Prevención |
| Huelga de trabajadores | Interrupción. Físico | Pérdida de tiempo de servicio. | (baja) | Brindar un entorno cómodo para el trabajo y mantener felices a los trabajadores. | Prevención |
| Ataque terrorista | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (baja) | Contar con copias de seguridad. | Prevención |
| Invasión alienígena | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (muy baja) | Contar con copias de seguridad. | Prevención |
| Un empleado trae a su hijo al trabajo y nos quita los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Intentar no traer familiares a la empresa, o tener una habitación donde puedan quedarse. | Prevención |
| Hay ratas y muerden los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Contratar servicios de empresas de fumigación y control de plagas. | Prevención |
| Se cae agua encima de los equipos | Interrupción. Físico | Pérdida de equipos e información. | (media alta) | Intentar beber en una zona habilitada para ello. | Prevención |
| En una visita guiada, la gente desconecta sin querer el servidor por tocar | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Intentar no acercar tanto a la visita a elementos tan importantes en la empresa. | Prevención |
| Escasez de chips | Interrupción. Físico | Impide mejorar y renovar los equipos temporalmente. | (alta) | Comprar más cantidad cuando no hay escasez. | Prevención |
| Transmisión de enfermedad contagiosa | Interrupción. Físico | Muchos empleados pueden enfermar (o morir), lo cual implica ausencias en los puestos de trabajo ocasionando demoras en la prestación de los servicios. | (alta) | Contar con medidas sanitarias además de la instalación de filtros purificadores de aire en espacios cerrados. | Prevención |
| Un empleado no autorizado entra a la sala de servidores y se dedica a desconectarlos | Interrupción.  Físico | Paro de servicios temporalmente. | (media) | Bloquear la puerta con un sistema en el que solo puedan acceder personas autorizadas. | Prevención |
| Durante la limpieza, el empleado tropieza con una torre y daña el equipo | Interrupción física | Daños en el equipo, pérdida de información. | (baja) | Tener cuidado, cambiar la distribución de los equipos. | Prevención |
| Se activa la alarma de incendios porque los empleados fuman a escondidas en el interior de la empresa y el agua de los aspersores daña los equipos | Interrupción. Físico | El humo de los cigarros puede dañar componentes internos de los equipos, además del agua de los aspersores. | (baja) | Informar a los empleados de que está prohibido fumar en el interior de la empresa, utilizar gas en lugar de agua en los aspersores anti-incendios. Vigilar a los empleados. | Prevención |
| A un empleado se le queda un cigarro encendido intentando esconderlo y provoca un incendio | Interrupción física | El fuego provoca la pérdida total de los servidores son poder recuperarlos. | (baja) | Informar a los empleados que está prohibido fumar en las instalaciones. Poner carteles para recordarlo. | Prevención |
| El techo de la empresa es deficiente y hay goteras | Interrupción física | Se filtra agua por las tuberías provocando humedades que terminaran en derrumbe del techo. | (muy bajo) | Revisión periódica de las instalaciones llamando al seguro. | Prevención |
| Un ex empleado vuelve a entrar en la empresa con el objetivo de causar el mayor daño posible por una venganza personal debido a un despido | Interrupción física y lógica | Puede romper componentes, apagar conexiones, robar material... | (bajo) | Retirar todas las llaves de acceso y tarjetas de identificación a los empleados una vez hayan abandonado la empresa. Contratar personal de seguridad. | Prevención |
| La rivalidad entre empleados provoca sabotajes | Interrupción física y lógica | Debido al deseo por demostrar su superioridad, algunos empleados pueden sabotear otros equipos con el fin de destacar entre sus compañeros. | (bajo) | Hacer saber que queremos a todos los empleados por igual y no hay ningún premio al más trabajador. | Prevención |
| La empresa subcontratada para la limpieza roba material | Interrupción Física | Pueden robar material imprescindible para el correcto funcionamiento de los equipos. | (muy bajo) | Instalar cámaras de seguridad, contratar personal para la vigilancia. | Prevención |
| Un empleado es asesinado | Interrupción física | Se paraliza la actividad de la empresa hasta que se aclare lo sucedido. | (muy bajo) | Tener cámaras de seguridad, seguridad dentro de las instalaciones. | Análisis forense |
| Un empleado se suicida | Interrupción física | Se detiene la actividad de la empresa hasta que se esclarezcan los motivos de dicho acto. | (muy baja) | Instalar un servicio psicológico en la empresa para supervisar la estabilidad de los empleados. | Prevención |
| Un empleado coge una baja y va a ausentarse durante bastante tiempo, estando su usuario disponible en la empresa | modificación lógica | Otros empleados pueden intentar acceder a su cuenta con el fin de dañarla o robar información. | (baja) | Deshabilitar las cuentas de empleados cuando vayan a ausentarse durante largos periodos de tiempo. | Prevención |
| La empresa es intervenida debido a que puede almacenar información sobre casos de corrupción del gobierno de Madrid | Interrupción física y lógica | La policía puede confiscar equipos y paralizar las actividades. | (media) | No se puede hacer nada. | - |
| Los empleados infectan los equipos de la empresa porque se dedican a navegar por la web libremente en su tiempo de trabajo | Interrupción lógica | Navegando por páginas no autorizadas y sin supervisión, los empleados pueden instalar sin saberlo, malware en los equipos. | (media) | Instalar bloqueadores de páginas web y supervisar las conexiones. | Prevención |
| El ex encargado del departamento de seguridad cambia las contraseñas con razón de un despido improcedente | Lógica | Imposibilita el acceso a muchas de las ramas de la empresa. | (media) | Tener copia de seguridad de todo y tener un sistema de recuperación de contraseñas llevado por más empleados de este departamento. | Prevención |
| Los empleados traen hamburguesas de fuera y comen encima de los equipos | Lógica | Las miguitas y las manchas pueden dañar componentes de los equipos. | (media) | Establecer una normativa para impedir que se coma justo encima de los ordenadores. | Prevención |
| Los equipos están cerca de la ventana, les da el sol y se calientan | Lógica | El calor excesivo del sol y el cristal pueden sobrecalentar los equipos provocando que funcionen más despacio o sufran daños. | (media/alta) | Poner todo a la sombra o bajar las persianas de las salas de los equipos | Prevención |
| Los empleados aprovechan las horas de trabajo para enchufar regletas con sus equipos personales de casa en los enchufes de los equipos de trabajo para cargar las baterías y ahorrar luz y sobrecargan la red de la empresa | Lógica | Añadiendo más carga energética de la planeada, la empresa puede sufrir cortes de luz, además que si los empleados desenchufan equipos de trabajo para poner las regletas, pueden ocasionar daños en la integridad o disponibilidad de los datos | (baja) | Establecer una política del uso de los enchufes de la empresa y vigilar que no suceda lo mencionado anteriormente | Prevención |
| Hay obras en el edificio y se produce un desalojo temporal indefinido | Interrupción logica y fisica | si no podemos entrar en el edificio, no se puede trabajar | (baja) | Habilitar la posibilidad de trabajar en remoto | Prevención mitigación |
| empleados de otras empresas se infiltran para robar información | lógica y física | otras empresas pueden enviar gente con el fin de infiltrarse para robar datos comprometedores y hundir la empresa | (baja) | Asegurarse de que se respetan los controles de acceso e investigar los perfiles de los empleados nuevos que se contratan | Prevención |
| Los empleados se escabullen al baño siempre que pueden para no trabajar | lógica | Si todos los empleados van al servicio constantemente, dejan desatendidos sus puestos de trabajo, lo que causa pausas en los servicios prestados por la empresa | (media) | Establecer turnos rotativos de 5 minutos para ir al baño | Prevención |

**Plan de seguridad - Frankfurt**

| **Ataque/**  **Amenaza** | **Categoría/**  **Tipo** | **Daño** | **Riesgo/**  **Probabilidad** | **Medida de seguridad** | **Categoría** |
| --- | --- | --- | --- | --- | --- |
| Incendio | Interrupción.  Físico | Pérdida total  de información. | ( baja) | Backup  externo,información en la nube. | Restauración |
| Explosión de gas | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Terremoto | Interrupción.  Físico | Pérdida total  de información. | (baja) | Backup  externo,información en la nube. | Restauración |
| Inundación | Interrupción.  Físico | Pérdida total  de información. | (media/alta) | Backup  externo,información en la nube. | Restauración |
| Volcán | Interrupción.  Físico | Pérdida total  de información. | ( baja) | Backup  externo,información en la nube. | Restauración |
| Fallo eléctrico | Interrupción.  Físico | Pérdida de unos minutos de trabajo,ya que tarda poco en volver la luz. | (baja) | Backup  externo,información en la nube. | Restauración |
| Tormenta de nieve | Interrupción. Físico | Posible pérdida de electricidad, inundación posterior e imposibilidad de acceso. | (media) | Backup  externo,información en la nube. | Restauración |
| Huracán | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Tornado | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Rayo | Interrupción. Físico | Pérdida de unos minutos de la información porque puede llegar a dejar sin luz a la empresa. | (media) | Trabajar online y que se guarde automático. | Restauración |
| Tsunami | Interrupción Físico | Pérdida de toda la información en los dispositivos de la empresa. | (nula) | Nada. | Prevención |
| Se abre una falla en el suelo y hunde la calle de la sede | Interrupción  Físico | Pérdida total de la información y del material de trabajo. | (muy baja) | Información en la nube. | Prevención |
| Tormenta de arena | Interrupción Físico | Pérdida de poca información,posible pérdida de ordenadores físicos. | (nula) | Información en la nube. | Prevención |
| Cae un árbol en la puerta de la empresa que impide el acceso al edificio | Interrupción. Físico | Imposibilita el acceso de los trabajadores a la empresa, lo que puede derivar en imposibilidad de solventar errores. | (muy baja) | Tener una puerta adicional en otro lado del edificio. Posibilidad de trabajo en remoto. | Prevención |
| Meteorito cae en la sede | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (baja) | Backup externo, información en la nube. | Restauración |
| Disturbios violentos | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| Derrumbamiento | Interrupción Física | Pérdida de toda la información en los dispositivos de la empresa. | (baja) | Backup externo, información en la nube. | Prevención o Restauración |
| Corrupción de documentos debido al uso de licencias pirata | Interrupción | Pérdida de información además de que aumenta la posibilidad de sufrir ataques. | (baja) | Uso de productos con licencias oficiales. | Prevención |
| Virus | Malware.Lógica | Detección de sistema, borrado de archivos y comportamientos erróneos. | (baja) | Antivirus, cortafuegos, copias de seguridad, análisis del sistema. | Prevención |
| Gusano | Malware. Lógica | Explotar errores de configuración de la red  bien explotar agujeros de seguridad en el sistema operativo y las aplicaciones. | (baja) | Análisis de programas,antivirus, software anti malware. | Prevención |
| Adware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (baja) | App lock. | Interrupción |
| Spyware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (baja) | Leer antes de aceptar las condiciones de páginas, tener actualizado el software. | Prevención |
| Keylogger | Malware. Lógica | Descifrar contraseñas y otra información ingresada con el teclado. | (baja) | Antivirus,copias de seguridad. | Prevención |
| Troyano | Malware. Lógica | Violaciones de privacidad, cómo usar la webcam, borrar el disco... | (baja) | Antivirus y análisis de dispositivos de entrada en el ordenador. | Prevención |
| Hijackers | Malware. Lógica | Modificación la redirección de los servidores DNS. | (baja) | Prestar especial atención a todo lo que instalamos en nuestro ordenador y qué sitios de internet estamos visitando. y servicios de hosting en los que podemos registrar un dominio seguro. | Prevención |
| Crackers | Malware. Lógica | Copia, rono, manipulación o eliminación de datos. | (media/baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Hackers | Malware. Lógica | Realizar muchos de los demás ataques nombrados como la activación de un virus, robo de información importante y modificación de las contraseñas establecidas. | (media) | Software, contraseñas distintas. | Prevención y modificación |
| Pharming | Malware. Lógica | Engaña a las víctimas para que entreguen credenciales de todo tipo de cuentas confidenciales, tales como correo electrónico, intranets corporativas y mucho más. | (baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Cookies | Malware. Lógica | No pueden infectar ordenadores con virus ni otro tipo de malware, pero algunos ciberataques secuestran las cookies y, por lo tanto, las sesiones de navegación. El peligro está en su capacidad de hacer un seguimiento de los historiales de navegación de las personas. | (muy alta) | App lock. | Prevención |
| Spam | Malware. Lógica | Puede causar daños significativos, infectando las computadoras de los usuarios con software malicioso capaz de dañar los sistemas y robar información personal. También puede consumir recursos de la red. | (muy alta) | No propagues los correos tipo ‘cadena’, utiliza la opción CCO, borra el encabezamiento**...** | Prevención |
| Hoaxes | Malware. Lógica | La pérdida de productividad, pérdida de credibilidad, saturación de redes locales y de mensajes. | (alta) | Estar atentos a temporales, faltas de ortografía y cadenas, usan imágenes de google... | Prevención y actuar de raiz |
| Doxing | Malware. Lógica | Conseguir información de la persona para así presionarla. No es un ataque en sí, consiste en recopilar información de las páginas web de las que el usuario entra. | (media) | No usar demasiadas redes sociales o evitar dar datos personales | Prevención |
| Phishing | Malware. Lógica | Manipular a la persona para que le de contraseñas,es decir, suplantar la identidad de una empresa.O obtener datos bancarios | (alta) | Tener cuidado con los correos o con la información que se envía,verificar la web donde se acceda | Prevención |
| Ping Flood | Malware. Lógica | Ping flood se basa en enviar a la víctima una cantidad abrumadora de paquetes ping. | (baja) | Tener un buen sistema operativo. | Prevención |
| Ping de la muerte | Malware. Lógica | El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. | (muy baja) | Casi todos los sistemas operativos de hoy en día rechazan esos paquetes. | Prevención |
| Escaneo de puertos | Malware. Lógica | Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles.  Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad. | (alta) | No abrir más puertos de los necesarios.Usar herramientas para comprobar los puertos abiertos.Utilizar cortafuegos.Equipos siempre actualizados. | Prevención y detección |
| ARP Spoofing | Malware. Lógica | ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo. | (alta) | Protegerse mediante los protocolos para consultar la IP | Prevención y detección |
| ACK flood | Malware. Lógica | Esta es una técnica para enviar un paquete TCP / ACK al objetivo a menudo con una dirección IP falsificada. | (media) | Usar cortafuegos para impedir el ataque | Prevención y detección |
| Ataque FTP Bounce | Malware. Lógica | El atacante puede conectarse a los servidores FTP y tiener la intención de enviar archivos a otros usuarios / máquinas que usan el comando PORT. Para que el servidor FTP intente enviar el archivo a otras máquinas en un puerto específico y verifique que el puerto esté abierto. | (media) | Deshabilitar el FTP estándar.Usar una encriptación potente y funciones hash | Prevención y detección |
| Ataque Man-In-The-Middle | Malware. Lógica | Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, sino que también pueden dirigir toda la información dentro de los dispositivos. | (alta) | Usar extensiones de correo de Internet seguras / multipropósito, o S / MIME.  Certificados de autenticación | Prevención. |
| ICMP Tunneling | Malware. Lógica | El tunneling se usa a menudo para eludir los firewalls que no bloquean los paquetes ICMP, o para establecer un canal de comunicación cifrado y difícil de rastrear entre dos computadoras sin interacción directa de la red. | (media) | Permitir a los administradores usar mensajes ICMP libremente.  Permitir el paso del gran tamaño de ICMP. | Prevención. |
| Ataque LOKI | Malware. Lógica | Este programa es una prueba de concepto que funciona para demostrar que los datos se pueden transmitir de forma secreta a través de una red escondiéndolos en el tráfico que normalmente no contiene cargas útiles. Se centra en el robo de datos bancarios, billeteras de criptomonedas y contraseñas de los navegadores web. | (medio) | Evitar abrir archivos de correo,porque se envía por ahí y es fundamental tener todo el paquete de office actualizado | Prevención. |
| Ataque de secuencia TCP | Malware. Lógica | Predice el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión. | (bajo) | Ahora mismo ya se han diseñado un algoritmo para generar números de secuencia aleatorios y que los atacantes no te los puedan adivinar | Prevención y detección |
| CAM Table Overflow | Malware. Lógica | La tabla CAM de un conmutador contiene información de red, como las direcciones MAC disponibles en los puertos físicos del conmutador y los parámetros de VLAN asociados. Los desbordamientos de la tabla CAM ocurren cuando una entrada de direcciones MAC se inunda en la tabla y se alcanza el umbral de la tabla CAM. Esto hace que el conmutador actúe como un concentrador, inundando la red con tráfico fuera de todos los puertos. | (medio) | Para prevenir este tipo de ataque, cambiaremos el puerto a un puerto de acceso emitiendo acceso en modo de puerto de conmutación. Luego asignaremos la cantidad máxima de direcciones MAC en las que se almacenará la tabla CAM para esta interfaz. | Prevención |
| Inyección SQL | Malware. Lógica | Ayuda al hacker a ejecutar un código debido a la presencia de vulnerabilidad en la capa de la base de datos de la Aplicación. En consecuencia, el código obtendrá datos confidenciales o incluso comprometerá la aplicación en sí. | (alto) | Limpiar las peticiones de caracteres especiales en SQL. Delimitar los valores en las consultas .Utilizar las últimas tecnologías.Escaneos regulares (con Acunetix) | Prevención |
| Cross-Site Request | Malware. Lógica | La falsificación de solicitudes entre sitios es un tipo de exploit malicioso de un sitio web mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. | (alto) | Navegar con atención y precaución.  Revisar el terminal en busca de malware.Protección frente a CSRF por parte del operario de la página web | Prevención y detección |
| Web Defacement | Malware. Lógica | La desfiguración del sitio web es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. | (alto) | Limitar los complementos de tu página web. Limitar los niveles de acceso. Escanear el código fuente de tu sitio | Prevención y detección |
| Buffer Overflow | Malware. Lógica | Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. | (medio) | Deshabilitar los servicios innecesarios. Proteja sus sistemas Linux, ya sea con un servidor de seguridad o un sistema de prevención de intrusiones basado en host (IPS). | Prevención y detección |
| Root kit | Malware. Lógica | El objetivo del atacante es obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. | (medio) | Instalar un sistema de seguridad.  Evitar abrir correos electrónicos de procedencia dudosa.  Evitar descargar archivos de sitios web extraños | Prevención |
| Caída de internet | Interrupción. Físico | Pérdida de tiempo de servicio. | (media) | Contar con varios proveedores de servicio de acceso a internet. | Prevención |
| Filtración de datos | Intercepción  Lógica | Los datos de los clientes pueden verse comprometidos. | (baja) | Implementar diversas medidas físicas y lógicas para evitar el acceso no autorizado a los datos. | Prevención |
| Averías físicas de los ordenadores | Interrupción. Físico | Pérdida de información, puede afectar al funcionamiento/rendimiento de un equipo. | (media) | Contar con personal de mantenimiento eficaz y reparación. | Prevención |
| Huelga de trabajadores | Interrupción. Físico | Pérdida de tiempo de servicio. | (baja) | Brindar un entorno cómodo para el trabajo y mantener felices a los trabajadores. | Prevención |
| Ataque terrorista | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (baja) | Contar con copias de seguridad. | Prevención |
| Invasión alienígena | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (muy baja) | Contar con copias de seguridad. | Prevención |
| Un empleado trae a su hijo al trabajo y nos quita los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Intentar no traer familiares a la empresa, o tener una habitación donde puedan quedarse. | Prevención |
| Hay ratas y muerden los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Contratar servicios de empresas de fumigación y control de plagas. | Prevención |
| Se cae agua encima de los equipos | Interrupción. Físico | Pérdida de equipos e información. | (media alta) | Intentar beber en una zona habilitada para ello. | Prevención |
| En una visita guiada, la gente desconecta sin querer el servidor por tocar | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Intentar no acercar tanto a la visita a elementos tan importantes en la empresa. | Prevención |
| Escasez de chips | Interrupción. Físico | Impide mejorar y renovar los equipos temporalmente. | (alta) | Comprar más cantidad cuando no hay escasez. | Prevención |
| Transmisión de enfermedad contagiosa | Interrupción. Físico | Muchos empleados pueden enfermar (o morir), lo cual implica ausencias en los puestos de trabajo ocasionando demoras en la prestación de los servicios. | (alta) | Contar con medidas sanitarias además de la instalación de filtros purificadores de aire en espacios cerrados. | Prevención |
| Un empleado no autorizado entra a la sala de servidores y se dedica a desconectarlos | Interrupción.  Físico | Paro de servicios temporalmente. | (media) | Bloquear la puerta con un sistema en el que solo puedan acceder personas autorizadas. | Prevención |
| Durante la limpieza, el empleado tropieza con una torre y daña el equipo | Interrupción física | Daños en el equipo, pérdida de información. | (baja) | Tener cuidado, cambiar la distribución de los equipos. | Prevención |
| Se activa la alarma de incendios porque los empleados fuman a escondidas en el interior de la empresa y el agua de los aspersores daña los equipos | Interrupción. Físico | El humo de los cigarros puede dañar componentes internos de los equipos, además del agua de los aspersores. | (baja) | Informar a los empleados de que está prohibido fumar en el interior de la empresa, utilizar gas en lugar de agua en los aspersores anti-incendios. Vigilar a los empleados. | Prevención |
| A un empleado se le queda un cigarro encendido intentando esconderlo y provoca un incendio | Interrupción física | El fuego provoca la pérdida total de los servidores son poder recuperarlos. | (baja) | Informar a los empleados que está prohibido fumar en las instalaciones. Poner carteles para recordarlo. | Prevención |
| El techo de la empresa es deficiente y hay goteras | Interrupción física | Se filtra agua por las tuberías provocando humedades que terminaran en derrumbe del techo. | (bajo) | Revisión periódica de las instalaciones llamando al seguro. | Prevención |
| Un ex empleado vuelve a entrar en la empresa con el objetivo de causar el mayor daño posible por una venganza personal debido a un despido | Interrupción física y lógica | Puede romper componentes, apagar conexiones, robar material... | (bajo) | Retirar todas las llaves de acceso y tarjetas de identificación a los empleados una vez hayan abandonado la empresa. Contratar personal de seguridad. | Prevención |
| La rivalidad entre empleados provoca sabotajes | Interrupción física y lógica | Debido al deseo por demostrar su superioridad, algunos empleados pueden sabotear otros equipos con el fin de destacar entre sus compañeros. | (bajo) | Hacer saber que queremos a todos los empleados por igual y no hay ningún premio al más trabajador. | Prevención |
| La empresa subcontratada para la limpieza roba material | Interrupción Física | Pueden robar material imprescindible para el correcto funcionamiento de los equipos. | (muy bajo) | Instalar cámaras de seguridad, contratar personal para la vigilancia. | Prevención |
| Un empleado es asesinado | Interrupción física | Se paraliza la actividad de la empresa hasta que se aclare lo sucedido. | (muy bajo) | Tener cámaras de seguridad, seguridad dentro de las instalaciones. | Análisis forense |
| Un empleado se suicida | Interrupción física | Se detiene la actividad de la empresa hasta que se esclarezcan los motivos de dicho acto. | (muy baja) | Instalar un servicio psicológico en la empresa para supervisar la estabilidad de los empleados. | Prevención |
| Un empleado coge una baja y va a ausentarse durante bastante tiempo, estando su usuario disponible en la empresa | modificación lógica | Otros empleados pueden intentar acceder a su cuenta con el fin de dañarla o robar información. | (baja) | Deshabilitar las cuentas de empleados cuando vayan a ausentarse durante largos periodos de tiempo. | Prevención |
| La empresa es intervenida debido a que puede almacenar información sobre casos de corrupción del gobierno de Madrid | Interrupción física y lógica | La policía puede confiscar equipos y paralizar las actividades. | (media) | No se puede hacer nada. | - |
| Los empleados infectan los equipos de la empresa porque se dedican a navegar por la web libremente en su tiempo de trabajo | Interrupción lógica | Navegando por páginas no autorizadas y sin supervisión, los empleados pueden instalar sin saberlo, malware en los equipos. | (media) | Instalar bloqueadores de páginas web y supervisar las conexiones. | Prevención |
| El ex encargado del departamento de seguridad cambia las contraseñas con razón de un despido improcedente | Lógica | Imposibilita el acceso a muchas de las ramas de la empresa. | (media) | Tener copia de seguridad de todo y tener un sistema de recuperación de contraseñas llevado por más empleados de este departamento. | Prevención |
| Los empleados traen hamburguesas de fuera y comen encima de los equipos | Lógica | Las miguitas y las manchas pueden dañar componentes de los equipos. | (media) | Establecer una normativa para impedir que se coma justo encima de los ordenadores. | Prevención |
| Los equipos están cerca de la ventana, les da el sol y se calientan | Lógica | El calor excesivo del sol y el cristal pueden sobrecalentar los equipos provocando que funcionen más despacio o sufran daños. | (media/alta) | Poner todo a la sombra o bajar las persianas de las salas de los equipos | Prevención |
| Los empleados aprovechan las horas de trabajo para enchufar regletas con sus equipos personales de casa en los enchufes de los equipos de trabajo para cargar las baterías y ahorrar luz y sobrecargan la red de la empresa | Lógica | Añadiendo más carga energética de la planeada, la empresa puede sufrir cortes de luz, además que si los empleados desenchufan equipos de trabajo para poner las regletas, pueden ocasionar daños en la integridad o disponibilidad de los datos | (baja) | Establecer una política del uso de los enchufes de la empresa y vigilar que no suceda lo mencionado anteriormente | Prevención |
| Hay obras en el edificio y se produce un desalojo temporal indefinido | Interrupción logica y fisica | si no podemos entrar en el edificio, no se puede trabajar | (baja) | Habilitar la posibilidad de trabajar en remoto | Prevención mitigación |
| empleados de otras empresas se infiltran para robar información | lógica y física | otras empresas pueden enviar gente con el fin de infiltrarse para robar datos comprometedores y hundir la empresa | (baja) | Asegurarse de que se respetan los controles de acceso e investigar los perfiles de los empleados nuevos que se contratan | Prevención |
| Los empleados se escabullen al baño siempre que pueden para no trabajar | lógica | Si todos los empleados van al servicio constantemente, dejan desatendidos sus puestos de trabajo, lo que causa pausas en los servicios prestados por la empresa | (media) | Establecer turnos rotativos de 5 minutos para ir al baño | Prevención |
| Los empleados en Oktoberfest deciden beber en exceso dentro de la oficina y no trabajan | lógica | Si los empleados están ebrios en horario de trabajo, las labores no se van a desarrollar correctamente | (baja) | Notificar que está prohibido beber alcohol en la empresa y menos encima de los equipos | Prevención |

**Plan de seguridad - Osaka**

| **Ataque/**  **Amenaza** | **Categoría/**  **Tipo** | **Daño** | **Riesgo/**  **Probabilidad** | **Medida de seguridad** | **Categoría** |
| --- | --- | --- | --- | --- | --- |
| Incendio | Interrupción.  Físico | Pérdida total  de información. | ( baja) | Backup  externo,información en la nube. | Restauración |
| Explosión de gas | Interrupción.  Físico | Pérdida total  de información. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Terremoto | Interrupción.  Físico | Pérdida total  de información. | (Alta) | Backup  externo,información en la nube. | Restauración |
| Inundación | Interrupción.  Físico | Pérdida total  de información. | (Alta) | Backup  externo,información en la nube. | Restauración |
| Volcán | Interrupción.  Físico | Pérdida total  de información. | (Bajo) | Backup  externo,información en la nube. | Restauración |
| Fallo eléctrico | Interrupción.  Físico | Pérdida de unos minutos de trabajo,ya que tarda poco en volver la luz. | (media) | Backup  externo,información en la nube. | Restauración |
| Tormenta de nieve | Interrupción. Físico | Posible pérdida de electricidad, inundación posterior e imposibilidad de acceso. | (media) | Backup  externo,información en la nube. | Restauración |
| Huracán | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (media) | Backup  externo,información en la nube. | Restauración |
| Tornado | Interrupción. Físico | Pérdida de toda la información en los dispositivos de la empresa. | (muy baja) | Backup  externo,información en la nube. | Restauración |
| Rayo | Interrupción. Físico | Pérdida de unos minutos de la información porque puede llegar a dejar sin luz a la empresa. | (muy baja) | Trabajar online y que se guarde automático. | Restauración |
| Tsunami | Interrupción Físico | Pérdida de toda la información en los dispositivos de la empresa. | (medio) | Nada. | Prevención |
| Se abre una falla en el suelo y hunde la calle de la sede | Interrupción  Físico | Pérdida total de la información y del material de trabajo. | (muy baja) | Información en la nube. | Prevención |
| Tormenta de arena | Interrupción Físico | Pérdida de poca información,posible pérdida de ordenadores físicos. | (muy baja) | Información en la nube. | Prevención |
| Cae un árbol en la puerta de la empresa que impide el acceso al edificio | Interrupción. Físico | Imposibilita el acceso de los trabajadores a la empresa, lo que puede derivar en imposibilidad de solventar errores. | (muy baja) | Tener una puerta adicional en otro lado del edificio. Posibilidad de trabajo en remoto. | Prevención |
| Meteorito cae en la sede | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| Disturbios violentos | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| Derrumbamiento | Interrupción Física | Pérdida de toda la información en los dispositivos de la empresa. | (baja) | Backup externo, información en la nube. | Prevención o Restauración |
| Corrupción de documentos debido al uso de licencias pirata | Interrupción | Pérdida de información además de que aumenta la posibilidad de sufrir ataques. | (baja) | Uso de productos con licencias oficiales. | Prevención |
| Virus | Malware.Lógica | Detección de sistema, borrado de archivos y comportamientos erróneos. | (alta) | Antivirus, cortafuegos, copias de seguridad, análisis del sistema. | Prevención |
| Gusano | Malware. Lógica | Explotar errores de configuración de la red  bien explotar agujeros de seguridad en el sistema operativo y las aplicaciones. | (alta) | Análisis de programas,antivirus, software anti malware. | Prevención |
| Adware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (alta) | App lock. | Interrupción |
| Spyware | Malware. Lógica | Puede afectar notablemente al funcionamiento/rendimiento de un equipo. | (baja) | Leer antes de aceptar las condiciones de páginas, tener actualizado el software. | Prevención |
| Keylogger | Malware. Lógica | Descifrar contraseñas y otra información ingresada con el teclado. | (baja) | Antivirus,copias de seguridad. | Prevención |
| Troyano | Malware. Lógica | Violaciones de privacidad, cómo usar la webcam, borrar el disco... | (baja) | Antivirus y análisis de dispositivos de entrada en el ordenador. | Prevención |
| Hijackers | Malware. Lógica | Modificación la redirección de los servidores DNS. | (baja) | Prestar especial atención a todo lo que instalamos en nuestro ordenador y qué sitios de internet estamos visitando. y servicios de hosting en los que podemos registrar un dominio seguro. | Prevención |
| Crackers | Malware. Lógica | Copia, rono, manipulación o eliminación de datos. | (media/baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Hackers | Malware. Lógica | Realizar muchos de los demás ataques nombrados como la activación de un virus, robo de información importante y modificación de las contraseñas establecidas. | (media) | Software, contraseñas distintas. | Prevención y modificación |
| Pharming | Malware. Lógica | Engaña a las víctimas para que entreguen credenciales de todo tipo de cuentas confidenciales, tales como correo electrónico, intranets corporativas y mucho más. | (baja) | Software, malware, antivirus, análisis del sistema,cortafuegos. | Prevención y modificación |
| Cookies | Malware. Lógica | No pueden infectar ordenadores con virus ni otro tipo de malware, pero algunos ciberataques secuestran las cookies y, por lo tanto, las sesiones de navegación. El peligro está en su capacidad de hacer un seguimiento de los historiales de navegación de las personas. | (muy alta) | App lock. | Prevención |
| Spam | Malware. Lógica | Puede causar daños significativos, infectando las computadoras de los usuarios con software malicioso capaz de dañar los sistemas y robar información personal. También puede consumir recursos de la red. | (muy alta) | No propagues los correos tipo ‘cadena’, utiliza la opción CCO, borra el encabezamiento**...** | Prevención |
| Hoaxes | Malware. Lógica | La pérdida de productividad, pérdida de credibilidad, saturación de redes locales y de mensajes. | (alta) | Estar atentos a temporales, faltas de ortografía y cadenas, usan imágenes de google... | Prevención y actuar de raiz |
| Doxing | Malware. Lógica | Conseguir información de la persona para así presionarla. No es un ataque en sí, consiste en recopilar información de las páginas web de las que el usuario entra. | (media) | No usar demasiadas redes sociales o evitar dar datos personales | Prevención |
| Phishing | Malware. Lógica | Manipular a la persona para que le de contraseñas,es decir, suplantar la identidad de una empresa.O obtener datos bancarios | (alta) | Tener cuidado con los correos o con la información que se envía,verificar la web donde se acceda | Prevención |
| Ping Flood | Malware. Lógica | Ping flood se basa en enviar a la víctima una cantidad abrumadora de paquetes ping. | (baja) | Tener un buen sistema operativo. | Prevención |
| Ping de la muerte | Malware. Lógica | El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. | (muy baja) | Casi todos los sistemas operativos de hoy en día rechazan esos paquetes. | Prevención |
| Escaneo de puertos | Malware. Lógica | Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles.  Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad. | (alta) | No abrir más puertos de los necesarios.Usar herramientas para comprobar los puertos abiertos.Utilizar cortafuegos.Equipos siempre actualizados. | Prevención y detección |
| ARP Spoofing | Malware. Lógica | ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo. | (alta) | Protegerse mediante los protocolos para consultar la IP | Prevención y detección |
| ACK flood | Malware. Lógica | Esta es una técnica para enviar un paquete TCP / ACK al objetivo a menudo con una dirección IP falsificada. | (media) | Usar cortafuegos para impedir el ataque | Prevención y detección |
| Ataque FTP Bounce | Malware. Lógica | El atacante puede conectarse a los servidores FTP y tiener la intención de enviar archivos a otros usuarios / máquinas que usan el comando PORT. Para que el servidor FTP intente enviar el archivo a otras máquinas en un puerto específico y verifique que el puerto esté abierto. | (media) | Deshabilitar el FTP estándar.Usar una encriptación potente y funciones hash | Prevención y detección |
| Ataque Man-In-The-Middle | Malware. Lógica | Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, sino que también pueden dirigir toda la información dentro de los dispositivos. | (alta) | Usar extensiones de correo de Internet seguras / multipropósito, o S / MIME.  Certificados de autenticación | Prevención. |
| ICMP Tunneling | Malware. Lógica | El tunneling se usa a menudo para eludir los firewalls que no bloquean los paquetes ICMP, o para establecer un canal de comunicación cifrado y difícil de rastrear entre dos computadoras sin interacción directa de la red. | (media) | Permitir a los administradores usar mensajes ICMP libremente.  Permitir el paso del gran tamaño de ICMP. | Prevención. |
| Ataque LOKI | Malware. Lógica | Este programa es una prueba de concepto que funciona para demostrar que los datos se pueden transmitir de forma secreta a través de una red escondiéndolos en el tráfico que normalmente no contiene cargas útiles. Se centra en el robo de datos bancarios, billeteras de criptomonedas y contraseñas de los navegadores web. | (medio) | Evitar abrir archivos de correo,porque se envía por ahí y es fundamental tener todo el paquete de office actualizado | Prevención. |
| Ataque de secuencia TCP | Malware. Lógica | Predice el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión. | (bajo) | Ahora mismo ya se han diseñado un algoritmo para generar números de secuencia aleatorios y que los atacantes no te los puedan adivinar | Prevención y detección |
| CAM Table Overflow | Malware. Lógica | La tabla CAM de un conmutador contiene información de red, como las direcciones MAC disponibles en los puertos físicos del conmutador y los parámetros de VLAN asociados. Los desbordamientos de la tabla CAM ocurren cuando una entrada de direcciones MAC se inunda en la tabla y se alcanza el umbral de la tabla CAM. Esto hace que el conmutador actúe como un concentrador, inundando la red con tráfico fuera de todos los puertos. | (medio) | Para prevenir este tipo de ataque, cambiaremos el puerto a un puerto de acceso emitiendo acceso en modo de puerto de conmutación. Luego asignaremos la cantidad máxima de direcciones MAC en las que se almacenará la tabla CAM para esta interfaz. | Prevención |
| Inyección SQL | Malware. Lógica | Ayuda al hacker a ejecutar un código debido a la presencia de vulnerabilidad en la capa de la base de datos de la Aplicación. En consecuencia, el código obtendrá datos confidenciales o incluso comprometerá la aplicación en sí. | (alto) | Limpiar las peticiones de caracteres especiales en SQL. Delimitar los valores en las consultas .Utilizar las últimas tecnologías.Escaneos regulares (con Acunetix) | Prevención |
| Cross-Site Request | Malware. Lógica | La falsificación de solicitudes entre sitios es un tipo de exploit malicioso de un sitio web mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. | (alto) | Navegar con atención y precaución.  Revisar el terminal en busca de malware.Protección frente a CSRF por parte del operario de la página web | Prevención y detección |
| Web Defacement | Malware. Lógica | La desfiguración del sitio web es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. | (alto) | Limitar los complementos de tu página web. Limitar los niveles de acceso. Escanear el código fuente de tu sitio | Prevención y detección |
| Buffer Overflow | Malware. Lógica | Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. | (medio) | Deshabilitar los servicios innecesarios. Proteja sus sistemas Linux, ya sea con un servidor de seguridad o un sistema de prevención de intrusiones basado en host (IPS). | Prevención y detección |
| Root kit | Malware. Lógica | El objetivo del atacante es obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. | (medio) | Instalar un sistema de seguridad.  Evitar abrir correos electrónicos de procedencia dudosa.  Evitar descargar archivos de sitios web extraños | Prevención |
| Caída de internet | Interrupción. Físico | Pérdida de tiempo de servicio. | (media) | Contar con varios proveedores de servicio de acceso a internet. | Prevención |
| Filtración de datos | Intercepción  Lógica | Los datos de los clientes pueden verse comprometidos. | (baja) | Implementar diversas medidas físicas y lógicas para evitar el acceso no autorizado a los datos. | Prevención |
| Averías físicas de los ordenadores | Interrupción. Físico | Pérdida de información, puede afectar al funcionamiento/rendimiento de un equipo. | (media) | Contar con personal de mantenimiento eficaz y reparación. | Prevención |
| Huelga de trabajadores | Interrupción. Físico | Pérdida de tiempo de servicio. | (baja) | Brindar un entorno cómodo para el trabajo y mantener felices a los trabajadores. | Prevención |
| Ataque terrorista | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (baja) | Contar con copias de seguridad. | Prevención |
| Invasión alienígena | Interrupción. Físico | Probablemente gran destrucción de la empresa en general, pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada, hasta pérdida de empleados. | (muy baja) | Contar con copias de seguridad. | Prevención |
| Un empleado trae a su hijo al trabajo y nos quita los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (baja) | Intentar no traer familiares a la empresa, o tener una habitación donde puedan quedarse. | Prevención |
| Hay ratas y muerden los cables | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Contratar servicios de empresas de fumigación y control de plagas. | Prevención |
| Se cae agua encima de los equipos | Interrupción. Físico | Pérdida de equipos e información. | (media alta) | Intentar beber en una zona habilitada para ello. | Prevención |
| En una visita guiada, la gente desconecta sin querer el servidor por tocar | Interrupción. Físico | Interrupción temporal de muchos de nuestros servicios y del uso de varias máquinas. | (media) | Intentar no acercar tanto a la visita a elementos tan importantes en la empresa. | Prevención |
| Escasez de chips | Interrupción. Físico | Impide mejorar y renovar los equipos temporalmente. | (alta) | Comprar más cantidad cuando no hay escasez. | Prevención |
| Transmisión de enfermedad contagiosa | Interrupción. Físico | Muchos empleados pueden enfermar (o morir), lo cual implica ausencias en los puestos de trabajo ocasionando demoras en la prestación de los servicios. | (alta) | Contar con medidas sanitarias además de la instalación de filtros purificadores de aire en espacios cerrados. | Prevención |
| Un empleado no autorizado entra a la sala de servidores y se dedica a desconectarlos | Interrupción.  Físico | Paro de servicios temporalmente. | (media) | Bloquear la puerta con un sistema en el que solo puedan acceder personas autorizadas. | Prevención |
| Durante la limpieza, el empleado tropieza con una torre y daña el equipo | Interrupción física | Daños en el equipo, pérdida de información. | (baja) | Tener cuidado, cambiar la distribución de los equipos. | Prevención |
| Se activa la alarma de incendios porque los empleados fuman a escondidas en el interior de la empresa y el agua de los aspersores daña los equipos | Interrupción. Físico | El humo de los cigarros puede dañar componentes internos de los equipos, además del agua de los aspersores. | (baja) | Informar a los empleados de que está prohibido fumar en el interior de la empresa, utilizar gas en lugar de agua en los aspersores anti-incendios. Vigilar a los empleados. | Prevención |
| A un empleado se le queda un cigarro encendido intentando esconderlo y provoca un incendio | Interrupción física | El fuego provoca la pérdida total de los servidores son poder recuperarlos. | (media) | Informar a los empleados que está prohibido fumar en las instalaciones. Poner carteles para recordarlo. | Prevención |
| El techo de la empresa es deficiente y hay goteras | Interrupción física | Se filtra agua por las tuberías provocando humedades que terminaran en derrumbe del techo. | (muy bajo) | Revisión periódica de las instalaciones llamando al seguro. | Prevención |
| Un ex empleado vuelve a entrar en la empresa con el objetivo de causar el mayor daño posible por una venganza personal debido a un despido | Interrupción física y lógica | Puede romper componentes, apagar conexiones, robar material... | (bajo) | Retirar todas las llaves de acceso y tarjetas de identificación a los empleados una vez hayan abandonado la empresa. Contratar personal de seguridad. | Prevención |
| La rivalidad entre empleados provoca sabotajes | Interrupción física y lógica | Debido al deseo por demostrar su superioridad, algunos empleados pueden sabotear otros equipos con el fin de destacar entre sus compañeros. | (bajo) | Hacer saber que queremos a todos los empleados por igual y no hay ningún premio al más trabajador. | Prevención |
| La empresa subcontratada para la limpieza roba material | Interrupción Física | Pueden robar material imprescindible para el correcto funcionamiento de los equipos. | (muy bajo) | Instalar cámaras de seguridad, contratar personal para la vigilancia. | Prevención |
| Un empleado es asesinado | Interrupción física | Se paraliza la actividad de la empresa hasta que se aclare lo sucedido. | (muy bajo) | Tener cámaras de seguridad, seguridad dentro de las instalaciones. | Análisis forense |
| Un empleado se suicida | Interrupción física | Se detiene la actividad de la empresa hasta que se esclarezcan los motivos de dicho acto. | (baja) | Instalar un servicio psicológico en la empresa para supervisar la estabilidad de los empleados. | Prevención |
| Un empleado coge una baja y va a ausentarse durante bastante tiempo, estando su usuario disponible en la empresa | modificación lógica | Otros empleados pueden intentar acceder a su cuenta con el fin de dañarla o robar información. | (baja) | Deshabilitar las cuentas de empleados cuando vayan a ausentarse durante largos periodos de tiempo. | Prevención |
| La empresa es intervenida debido a que puede almacenar información sobre casos de corrupción del gobierno de Madrid | Interrupción física y lógica | La policía puede confiscar equipos y paralizar las actividades. | (media) | No se puede hacer nada. | - |
| Los empleados infectan los equipos de la empresa porque se dedican a navegar por la web libremente en su tiempo de trabajo | Interrupción lógica | Navegando por páginas no autorizadas y sin supervisión, los empleados pueden instalar sin saberlo, malware en los equipos. | (media) | Instalar bloqueadores de páginas web y supervisar las conexiones. | Prevención |
| El ex encargado del departamento de seguridad cambia las contraseñas con razón de un despido improcedente | Lógica | Imposibilita el acceso a muchas de las ramas de la empresa. | (media) | Tener copia de seguridad de todo y tener un sistema de recuperación de contraseñas llevado por más empleados de este departamento. | Prevención |
| Los empleados traen hamburguesas de fuera y comen encima de los equipos | Lógica | Las miguitas y las manchas pueden dañar componentes de los equipos. | (media) | Establecer una normativa para impedir que se coma justo encima de los ordenadores. | Prevención |
| Los equipos están cerca de la ventana, les da el sol y se calientan | Lógica | El calor excesivo del sol y el cristal pueden sobrecalentar los equipos provocando que funcionen más despacio o sufran daños. | (media/alta) | Poner todo a la sombra o bajar las persianas de las salas de los equipos | Prevención |
| Los empleados aprovechan las horas de trabajo para enchufar regletas con sus equipos personales de casa en los enchufes de los equipos de trabajo para cargar las baterías y ahorrar luz y sobrecargan la red de la empresa | Lógica | Añadiendo más carga energética de la planeada, la empresa puede sufrir cortes de luz, además que si los empleados desenchufan equipos de trabajo para poner las regletas, pueden ocasionar daños en la integridad o disponibilidad de los datos | (baja) | Establecer una política del uso de los enchufes de la empresa y vigilar que no suceda lo mencionado anteriormente | Prevención |
| Hay obras en el edificio y se produce un desalojo temporal indefinido | Interrupción logica y fisica | si no podemos entrar en el edificio, no se puede trabajar | (baja) | Habilitar la posibilidad de trabajar en remoto | Prevención mitigación |
| empleados de otras empresas se infiltran para robar información | lógica y física | otras empresas pueden enviar gente con el fin de infiltrarse para robar datos comprometedores y hundir la empresa | (baja) | Asegurarse de que se respetan los controles de acceso e investigar los perfiles de los empleados nuevos que se contratan | Prevención |
| Los empleados se escabullen al baño siempre que pueden para no trabajar | lógica | Si todos los empleados van al servicio constantemente, dejan desatendidos sus puestos de trabajo, lo que causa pausas en los servicios prestados por la empresa | (media) | Establecer turnos rotativos de 5 minutos para ir al baño | Prevención |

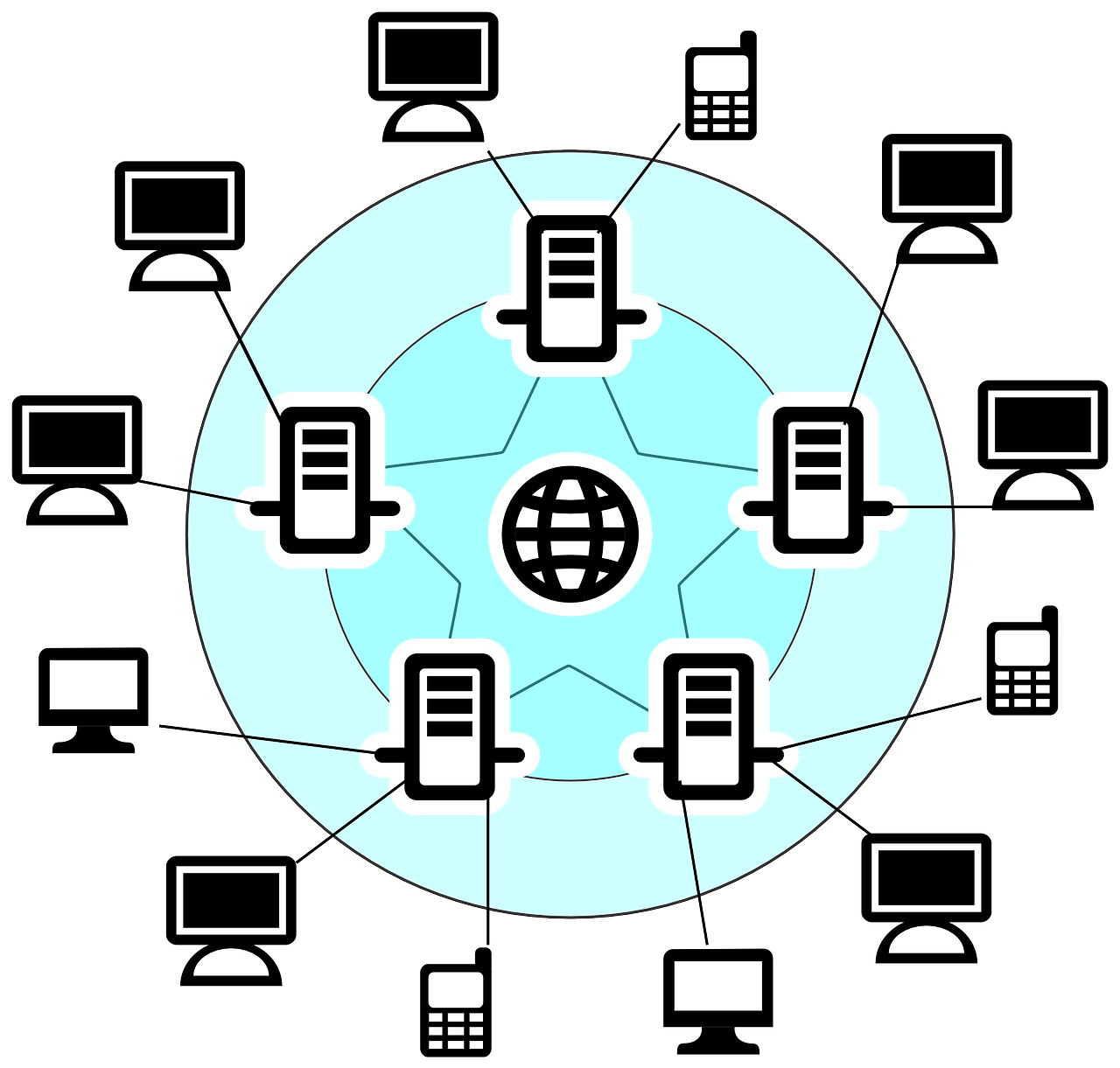
**PLAN DE CONTINGENCIA**

****

**EJEMPLOS LÓGICAS**

***Los siguientes casos son ejemplos que impartiríamos gracias a nuestro plan de contingencia de forma lógica:***

| ARP Spoofing | Malware. Lógica | ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo. | (alta) | Protegerse mediante los protocolos para consultar la IP | Prevención y detección |
| --- | --- | --- | --- | --- | --- |



***En caso de llegar a suceder, nos encargaríamos de subdividir la red para que no llegase a afectar a todos los equipos para así poner en “cuarentena” solo una parte de la red y no todo, por lo que nos sería más fácil encontrar por donde se intentan infiltrar.***

| Doxing | Malware. Lógica | Conseguir información de la persona para así presionarla. No es un ataque en sí, consiste en recopilar información de las páginas web de las que el usuario entra. | (media) | No usar demasiadas redes sociales o evitar dar datos personales | Prevención |
| --- | --- | --- | --- | --- | --- |

***En caso de que esto sucediese lo que haríamos sería intentar buscar donde están las fugas de datos para poder corregirlo y seguidamente buscaríamos por la red lo máximo posible donde se publican nuestros datos para poder denunciarlo.***

| Gusano | Malware. Lógica | Explotar errores de configuración de la red  bien explotar agujeros de seguridad en el sistema operativo y las aplicaciones. | (baja) | Análisis de programas,antivirus, software anti malware. | Prevención |
| --- | --- | --- | --- | --- | --- |

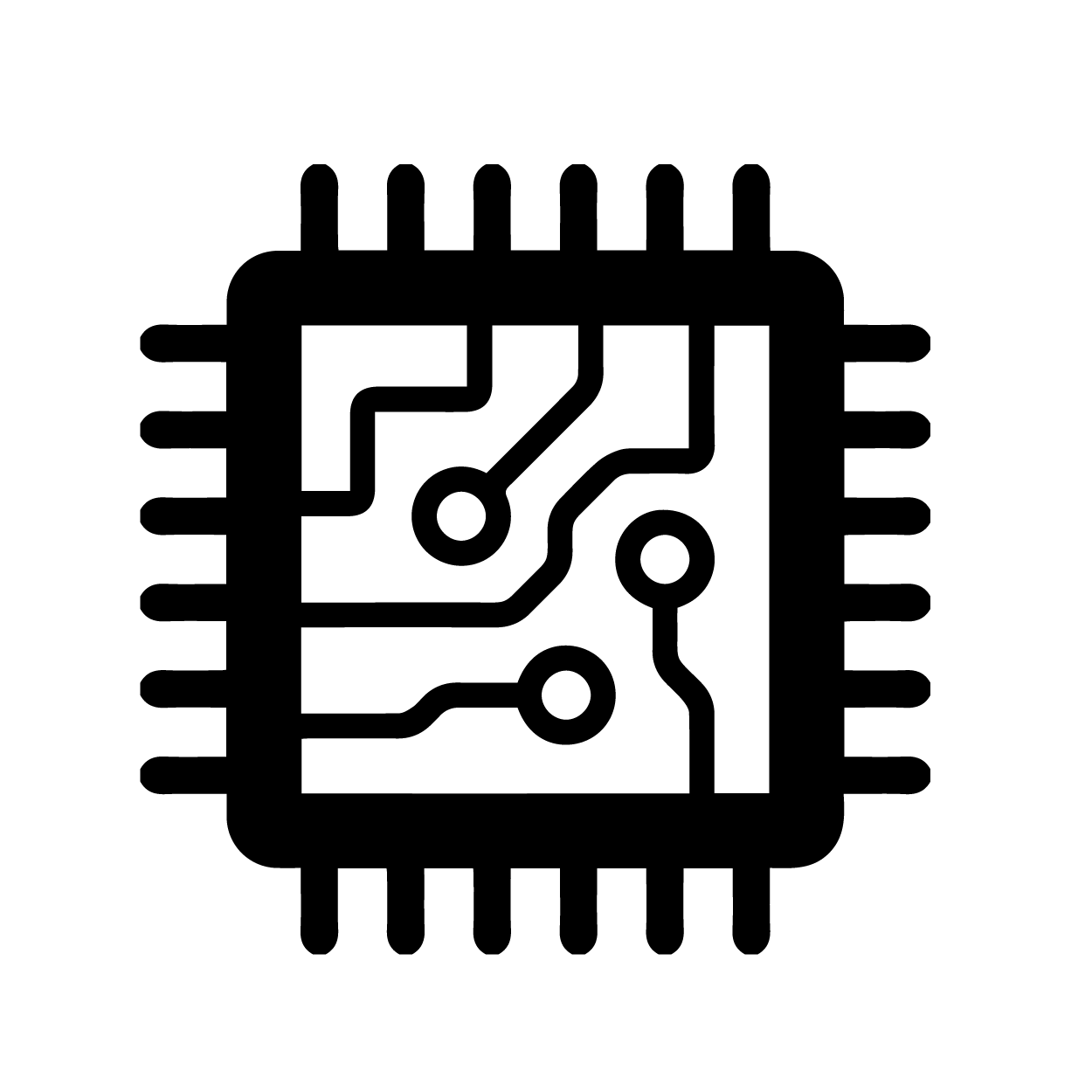
***Si el equipo se infectase con un Gusano informático lo que haríamos sería usar los mejores antivirus del mercado para así poder eliminarlo por completo de nuestros sistemas.***

**EJEMPLOS FÍSICOS**

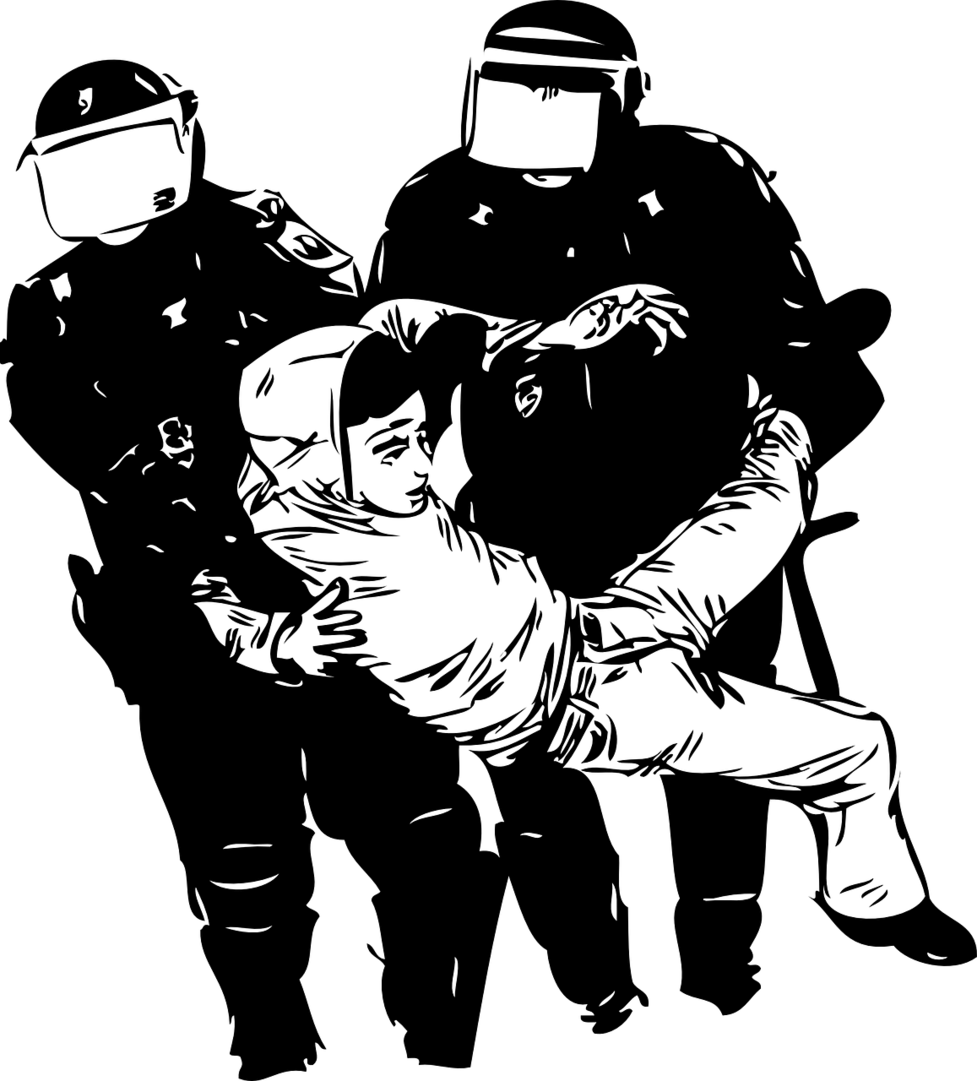
***Los siguientes casos son ejemplos que impartiríamos gracias a nuestro plan de contingencia de forma lógica:***

| Escasez de chips | Interrupción. Físico | Impide mejorar y renovar los equipos temporalmente. | (alta) | Comprar más cantidad cuando no hay escasez. | Prevención |
| --- | --- | --- | --- | --- | --- |



***En caso de que ocurriera esta situación, se recurrirá a alternativas más cercanas como comprar temporalmente equipos antiguos de los que podamos rescatar chips y para aprovechar otros componentes, hasta que haya nuevos suministros.***

| Disturbios violentos | Interrupción Física | Pérdida de equipos (ordenadores, discos duros) a causa de los daños y desperfectos de fachada. | (media) | Backup externo, información en la nube. | Restauración |
| --- | --- | --- | --- | --- | --- |



***En este caso, se intentará recuperar lo posible, y reparar daños físicos al igual que recurrir a medidas legales junto con el departamento de abogados para recurrir al estado una indemnización por los daños causados tanto en ese momento como a posteriori por la productividad que habremos perdido.***

| Un empleado se suicida | Interrupción física | Se pierde a un empleado y el rendimiento se vería reducido. | (baja) | Instalar un servicio psicológico en la empresa para supervisar la estabilidad de los empleados. | Prevención |
| --- | --- | --- | --- | --- | --- |

***Si sucediese esto se detendría la actividad de la empresa hasta que se esclarezcan los motivos de dicho acto y acto seguido se buscaría un reemplazo para la vacante libre.***