Plan Director de Seguridad

Grupo 4: Rodilla

Adrián tenorio

Gonzalo Pascual

Luca Sancho

Lucas Gavín

Tomás Rodríguez

Histórico de revisiones

Versión	Fecha	Autor de la Revisión	Resumen de Cambios
1.0	25/10/2023	Rodilla UFV	Se ha creado el documento

Distribución

Nombre	Posición

Aprobación

Nombre	Posición	Firma	Fecha

Índice

1. Introducción

Un Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

Es un documento dinámico que debe revisarse y actualizarse periódicamente para mantenerse al día con las amenazas emergentes y los cambios en el entorno empresarial. También sirve como una guía estratégica para garantizar que la seguridad de la organización esté alineada con sus objetivos y valores.

1.1 Contexto de la empresa

Somos una franquicia de Rodilla, ubicada en el campus universitario Francisco de Victoria en la localidad de Majadahonda.

- **Local:** tenemos un almacén de comida y despacho para el encargado dentro del local. Además, disponemos de comedor interno, donde está ubicada la barra donde se realizan los pedidos y terraza para los comensales. Dentro de la barra están las cámaras para almacenar las bebidas, conectando con la cocina.

- **Empleados:** la plantilla está formada por el encargado, cuya función es gestionar los productos y pedidos desde su despacho, y ayudar dependiendo de la situación. Hay un cocinero y un camarero en la barra donde se toma nota. Y un último empleado que trabaja según la demanda del momento, puede estar actuando tanto de pinche de cocina, como de camarero.

- **Horarios:** nuestro horario es de lunes a viernes de 10:00 a 18:00, por lo cual disponemos de desayuno y comida.

- **Dispositivos:** dentro del despacho hay un ordenador usado por el encargado para realizar la organización y gestión de los alimentos mediante los servicios de la organización Rodilla. En la barra está ubicada la caja donde se realizan los pedidos y los TPV para el pago de los clientes. Respecto al acceso a internet, tenemos dos routers. Uno de acceso gratuito para los clientes, y otro para la red privada de la corporativa que utilizaran los empleados.

- **Software:** utilizaremos tres aplicaciones distintas. La primera, es la aplicación que usa la caja para seleccionar qué comida hay que preparar y que llegue al cocinero mediante una comanda. La segunda, es la aplicación que usará el encargado para

gestionar la temperatura tanto de las cámaras como del almacén. Y la última, una aplicación para el sistema de fichaje de los empleados.

El objetivo principal de este plan director de seguridad es garantizar la protección de los activos, la información y la seguridad de los empleados y clientes de Rodilla en el campus universitario. Por lo que, este plan director abarca los siguientes aspectos de seguridad:

- Seguridad de los clientes y empleados
- Seguridad de los datos de tarjetas de crédito y otros datos sensibles
- Protección de activos físicos, incluyendo el almacenamiento con refrigeración
- Seguridad de las redes inalámbricas (Wi-Fi)

1.2 Estudio de mercado

Nuestro local se enfoca en el sector de la hostelería, ofreciendo tanto servicio de desayuno, como de comida. El producto va dirigido a cualquier persona indistintamente de su género y de su edad. No obstante, debido a que nos localizamos dentro de un campus universitario, la mayoría de nuestro público comprende entre un rango de edad entre 18 y 30 años. También nos regimos por los horarios de la universidad y el horario laboral está enfocado en las horas donde más estudiantes o profesores pueden venir a nuestro local, de 10:00 a 18:00.

En el caso del campus universitario Francisco de Vitoria, dispone de más locales que sirven alimentación. Sin embargo, nuestra ubicación favorece el negocio al estar ubicada en el medio del campus, y nuestro rango de precios es accesible para cualquier comensal con un precio medio de comida por persona de 10€. El precio está basado tanto en el valor económico de la producción y elaboración de la comida, como de la influencia de los precios de los demás establecimientos de comida del campus.

2. Seguridad de la empresa

Para mantener la seguridad de los activos, nos vamos a centrar en distintos puntos que determinarán la seguridad de dichos activos.

2.1 Políticas de Seguridad

Se establecerán políticas y procedimientos de seguridad, que incluyen:

- **Acceso restringido al almacenamiento y áreas sensibles**:

En nuestro caso, tanto la puerta del despacho del encargado, como la puerta del almacén dispondrán de un panel con contraseña de tipo PIN para su acceso.

- **Procedimientos de pago seguros y cumplimiento de los estándares PCI DSS para proteger los datos de tarjetas de crédito:**

El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) es un estándar de seguridad de la información reconocido internacionalmente diseñado específicamente para aplicarse a organizaciones que manejan datos de tarjetas de crédito. Para ello, cumpliremos los requisitos que se proponen en dicho estándar.

- **Políticas de contraseñas y autenticación para las redes Wi-Fi:**

Respecto a las contraseñas que se utilizaran en la empresa, ya sea en las app, en la wifi o en el mismo ordenador del encargado, seguirán estas políticas:

Longitud y complejidad: se deben establecer contraseñas con una longitud mínima de 12 caracteres, con una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

Evitar información personal: se prohíbe el uso de nombres, fechas de nacimiento o información personal fácilmente accesible en las contraseñas.

Cambio regular: las contraseñas se cambiarán cada 60 días, para evitar el uso continuo de contraseñas comprometidas.

Bloqueo de intentos de acceso: se van a implementar medidas para bloquear temporalmente las cuentas después de varios intentos fallidos de inicio de sesión para prevenir ataques de fuerza bruta.

En la parte de autenticación de la red Wifi, se utilizarán una serie de políticas para mejorar la seguridad:

WPA2: se va a utilizar el protocolo de seguridad WPA2.

Filtrado de direcciones MAC: se permitirán únicamente dispositivos específicos mediante el filtrado de direcciones MAC.

Redes separadas para clientes: se va a configurar una red Wi-Fi separada para invitados con una contraseña diferente, limitando el acceso a los recursos de la red principal.

Certificados y autenticación de dos factores (2FA): se implementarán certificados para autenticación en la redes corporativas y la autenticación de dos factores (contraseña + código enviado al teléfono móvil).

Actualizaciones y parches: se mantendrá actualizado el firmware del enrutador para asegurar que las vulnerabilidades conocidas esten parcheadas.

Monitoreo y registro: configuraremos registros de actividad y monitoreo para identificar patrones inusuales o intentos de acceso no autorizados.

- **Políticas de seguridad de la información:**

Las políticas de seguridad de la información son directrices y procedimientos diseñados para proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Para ello se seguirán diversas políticas de seguridad de la información para garantizar la seguridad de los datos y protegerse contra amenazas internas y externas.

2.2 Acceso a las Instalaciones

Se implementarán medidas de seguridad para el acceso a las instalaciones, que consta de sistemas de videovigilancia, sistema de alarma ante accesos no autorizados y controles de acceso a las instalaciones sensibles del local. Dispondremos de un par de cámaras a la entrada del local, así como en los puntos de acceso al despacho del encargado y al almacén. La alarma se ubica en el interior del establecimiento y se pondrá en funcionamiento en los horarios no laborables. Como seguridad adicional, se podrá acceder tanto al almacén como al despacho mediante una contraseña tipo PIN que habrá en las puertas.

2.3 Seguridad de los TPV

Se garantizará que los terminales de punto de venta (TPV) estén protegidos contra manipulaciones y que cumplan con los estándares de seguridad para transacciones con tarjetas de crédito.

Un TPV es una terminal punto de venta, es un dispositivo que, en un establecimiento comercial, permite gestionar tareas relacionadas, con la venta y permite, gracias a los datafonos, el cobro por tarjeta de crédito o débito, la creación e impresión del ticket de venta , gestionar el inventario o generar informes que ayudan a la gestión del negocio, entre otras.

Los TPV se componen de hardware (dispositivos físicos) y software (sistema operativo y programa de gestión).

Medidas de seguridad para el tpv:

- **Seguridad física**:

Ubicación Segura: se colocará el TPV en un lugar seguro y de difícil acceso para personas no autorizadas.

Cierre físico: se utilizaran cerraduras y candados para proteger el hardware del TPV.

- **Seguridad de la red**:

Firewall: se utilizará un firewall para proteger la red del TPV contra amenazas externas.

Conexión Segura: nos aseguraremos de que la conexión a internet sea segura y encriptada, preferiblemente a través de una red privada virtual (VPN).

Actualizaciones de software: mantendremos el software del TPV actualizado para corregir vulnerabilidades conocidas.

- **Seguridad de los datos**:

Encriptación de datos: nos aseguraremos de que los datos transmitidos entre el TPV y el servidor estén encriptados para proteger la información financiera.

Almacenamiento seguro: guardaremos los datos sensibles de los clientes y las transacciones de manera segura, utilizando métodos de almacenamiento cifrado.

- **Autenticación y control de acceso**:

Contraseñas seguras: el TPV tendrá contraseñas robustas y se cambiarán regularmente.

Autenticación de dos factores: implementaremos la autenticación de dos factores para agregar una capa adicional de seguridad.

- **Monitoreo y registro de actividades**:

Llevaremos un registro de todas las actividades relacionadas con el TPV, incluyendo transacciones, accesos y cambios en la configuración.

Utilizaremos sistemas de monitoreo de seguridad para detectar actividades sospechosas.

- **Protección contra malware y virus**:

El TPV tendrá instalado software de seguridad actualizado y confiable para proteger contra malware y virus.

- **Plan de respuesta a incidentes**:

Desarrollaremos un plan de respuesta a incidentes que describa cómo actuar en caso de una brecha de seguridad o un problema con el TPV.

- **Cumplimiento con estándares de seguridad**:

Nos aseguraremos de cumplir con las regulaciones de seguridad de datos aplicables, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago.

- **Actualización y reemplazo**:

Actualizaremos o reemplazaremos el hardware y el software del TPV cuando sea necesario para garantizar que se mantenga seguro y compatible con los estándares actuales.

Para proteger estos datos sensibles , los TPV estan equipados con medidas de seguridad que incluyen cortafuegos, detección de intrusiones, software de prevención y técnicas de encriptación.

2.4 Seguridad de Red

La seguridad de las redes del local se asegurarán mediante:

- **Encriptación de datos:**

Habilitaremos el protocolo de encriptación WPA2 en el router para asegurar la comunicación inalámbrica entre dispositivos y utilizaremos contraseñas robustas. El protocolo WPA2 es un protocolo cifrado de seguridad que protege el tráfico de Internet en redes inalámbricas. La segunda generación del protocolo de seguridad de Acceso protegido Wi-Fi (WPA2) aborda errores anteriores y ofrece un cifrado más potente.

- **Autenticación sólida:**

Estableceremos una autenticación sólida, implementando medidas que aseguren la identidad y seguridad tanto de los empleados como de los clientes. Aquí va nuestra propuesta:

Sistema de credenciales:

Empleados: cada empleado tendrá su propia identificación única (por ejemplo, tarjetas de acceso, códigos PIN) para ingresar al local y para acceder a áreas restringidas.

Encargado: tendrá un nivel de acceso superior y estará a cargo de la administración de las credenciales.

Cámaras de seguridad:

Se instalarán cámaras de seguridad visibles en áreas clave del local para disuadir la actividad delictiva y para proporcionar pruebas en caso de incidentes.

Además de instalar un sistema de alarma que se active fuera del horario de funcionamiento normal.

Control de acceso físico:

Implementaremos cerraduras de alta calidad y seguras en todas las entradas y salidas. Sobre todo, sistemas de cerraduras electrónicas basadas en contraseña PIN, que permiten un mayor control.

Limitaremos el acceso a la caja registradora solo a personal autorizado y designaremos a una persona de confianza para manejar el efectivo.

Educación y concienciación del personal:

Capacitaremos al personal sobre la importancia de la encriptación y las mejores prácticas para mantener la seguridad de los datos.

- **Actualizaciones regulares del firmware:**

Para mantener el firmware actualizado proponemos ciertas pautas:

Programa de mantenimiento regular:

Establecer un programa de mantenimiento regular que incluya la actualización de firmware como una tarea programada.

Notificaciones automatizadas:

Configurar notificaciones automáticas para informarnos sobre actualizaciones disponibles tan pronto como estén disponibles.

Queremos que el cliente se preocupe lo menos posible sobre las actualizaciones de firmware ya que esa es nuestra labor así que las automatizamos lo máximo posible y tendrán la capacidad de autogestionarse con launchers fáciles para actualizarlos ellos mismos en caso de fallo.

- **Instalar un firewall**

Hardware y software del firewall:

Elegimos un firewall adecuado para el tamaño y las necesidades del local. Trabajaremos con un firewall que se ejecute en un servidor.

Configuración básica del firewall:

Se establecen reglas de firewall para permitir o bloquear el tráfico según las necesidades.

- **Seguridad de Red:**

La red incluirá segmentos o subredes separadas que estén aisladas lógicamente unas de otras. Se utilizarán tecnologías de red, como los firewalls, para lograr la segmentación.

Se implementarán VPNs (Redes Privadas Virtuales) y autenticación de doble factor para proteger las conexiones remotas.

2.5 Seguridad en las aplicaciones

- **Aplicación de fichaje:**

Será una aplicación en la que el usuario podrá entrar con su cuenta, ver sus datos de fichaje y fichar a su hora de entrada y de salida del puesto de trabajo. Esta información será compartida al servidor donde se guardaran los datos de todos los empleados

- **Aplicación de monitorización y control de las cámaras y almacén:**

En esta aplicación los empleados solo podrán ver la temperatura del almacén sin cambiar nada, mientras que el encargado podrá gestionar tanto de las cámaras como la temperatura del almacén. Toda la información se compartirá al servidor donde se guarden todos los datos.

- **Aplicación de pedidos:**

Esta aplicación será con la que los empleados hagan los pedidos de los clientes para mandarlos a cocina y que se preparen. Esta aplicación no tendrá distinción de roles y todos los empleados podrán utilizarla. Todos los pedidos se mandarán al servidor donde se guarden los registros.

Las aplicaciones están instaladas en teléfonos de la empresa designados específicamente para ellas en las que no se podrá instalar, ni usar nada más para de esta forma protegerlas más por lo que será necesario tener en cuenta los siguientes puntos de seguridad:

- **Gestión de dispositivos móviles (MDM):**

Implementaremos una solución de gestión de dispositivos móviles (MDM (Mobile Device Management)) para administrar y controlar los dispositivos de manera centralizada. Esto permite la aplicación de políticas de seguridad, la distribución de aplicaciones y actualizaciones, y la capacidad de borrar datos en caso de pérdida o robo. Para ello habrá que buscar cual MDM va mejor para nuestras necesidades como puede ser MobileIron, VMware Workspace ONE e implementarlo.

- **Seguridad física:**

Se protegerán físicamente los dispositivos móviles para evitar su manipulación o robo. Se utilizarán carcasas seguras y un cajón con pin al igual que el almacén.

Se ejecutarán versiones actualizadas y seguras del sistema operativo y firmware para que estén al día y así evitar vulnerabilidades.

- **Autenticación y control de acceso:**

En todas las aplicaciones se implementará una autenticación segura para que solo el personal autorizado pueda acceder a la aplicación con su cuenta.

Se establecerán roles y permisos para garantizar que los empleados solo tengan acceso a las funciones necesarias para su trabajo. Los empleados tendrán solo información sobre su cuenta mientras que el encargado tendrá cierta información sobre los empleados.

- **Cifrado de Datos:**

Para proteger los datos almacenados en los dispositivos móviles, vamos a utilizar el cifrado de datos en reposo. Esto implica cifrar los datos antes de que se almacenen en la memoria del dispositivo.

La aplicación se comunicará con un servidor o una base de datos remota, por lo que las comunicaciones habrá que protegerlas mediante protocolos seguros como HTTPS y cifrados de extremo a extremo para garantizar que los datos sean seguros durante la transmisión entre la aplicación y el servidor.

- **Protección contra Amenazas:**

Se utilizarán medidas de seguridad contra ataques comunes, como inyecciones SQL que son un tipo de ataque en el que un atacante introduce código SQL malicioso en las entradas de una aplicación, lo que puede permitirle acceder o manipular la base de datos de la aplicación. Para ello se validará y filtrará todas las entradas de datos del usuario para garantizar que no contengan caracteres SQL maliciosos.

2.6 Formación y Concienciación

- **Programas de Formación:**

Estableceremos un programa de formación continua para todo el personal, centrándonos en los siguientes aspectos: Mejores prácticas en el uso de dispositivos móviles, ordenadores o aplicaciones corporativas; formación acerca de la seguridad de la información y de la identificación de correos electrónicos o enlaces maliciosos, así como la importancia del uso de contraseñas seguras. Se dará también formación a los empleados para establecer un plan de respuesta a incidentes, en el que se describa cómo se gestionan y comunican ciertos incidentes de seguridad

- **Concienciación:**

Se implementarán campañas de concienciación regulares para fomentar una buena cultura de la seguridad entre los empleados. Se realizan distintos tipos de pruebas, como por ejemplo de phishing, para evaluar la preparación de los empleados.

- **Seguimiento y Evaluación:**

Quedará establecido un proceso de evaluaciones periódicas para medir y mejorar el nivel de conocimiento y cumplimiento del personal en seguridad de la información. Se ajustarán los programas de formación y concienciación en función de los resultados.

2.7 Auditorías y Revisiones

Estableceremos políticas de seguridad de la información que incluyan directrices claras sobre el uso de dispositivos móviles, ordenadores, TPVs y acceso a datos. Se hará especial hincapié en las revisiones de seguridad de los sistemas informáticos y en sus infraestructuras tecnológicas para asegurarse de que estén alineados con las políticas de seguridad. Se desarrollarán planes de mitigación en caso de que se identifiquen vulnerabilidades o incumplimientos de políticas

- **Auditorías Internas:**

Programación de auditorías internas regulares para revisar el cumplimiento de las políticas de seguridad y de todas las regulaciones o leyes aplicables (como la protección de datos personales). El objetivo principal de estas es identificar y corregir posibles brechas de seguridad y áreas de mejora.

- **Auditorías Externas:**

Contratar servicios de auditoría externa para realizar evaluaciones imparciales de la seguridad de la información y la conformidad con estándares de seguridad relevantes.

3. Análisis de riesgos

El propósito fundamental de este análisis es proporcionar una visión completa de los riesgos a los que se enfrenta la franquicia de Rodilla, con el fin de establecer estrategias y medidas de mitigación adecuadas que permitan garantizar la seguridad de los clientes, proteger los activos y mantener la operación fluida y exitosa.

En los siguientes puntos, se explorarán los activos, las amenazas y riesgos potenciales que podrían afectar a la empresa y se propondrán soluciones y estrategias para mitigarlos y garantizar la seguridad, el cumplimiento normativo y la continuidad del negocio.

3.1 Identificación de activos

En un establecimiento de comida como Rodilla, existen varios activos esenciales y capas de activos relacionados con la operación. A continuación, se detallan estos activos en capas, donde las capas superiores dependen de las inferiores:

- **Activos esenciales:**

Información que se maneja: menú, inventario de alimentos y registros de ventas.

Servicios prestados: servicio de comida, comedor interior, terraza, pedidos y entrega de alimentos.

- **Equipamiento informático:**

Aplicaciones (Software): aplicación de pedidos, aplicación de monitorización y control de las cámaras y almacén, aplicación de fichaje de empleados.

Equipos Informáticos (Hardware): ordenador del encargado, TPV y caja en la barra.

Comunicaciones: red privada para empleados, red pública para clientes.

Soportes de información: almacenamiento de datos de ventas y pedidos.

- **Entorno:**

Equipamiento y suministros: energía y climatización.

Mobiliario: sillas, mesas, sombrillas.

- **Servicios subcontratados a terceros:**

  Mantenimiento de equipos, servicios de internet y proveedores de alimentación.

- **Instalaciones físicas:**

  Cocina, área de comedor, terraza, despacho y almacén.

- **Personal:**

  Encargado, cocineros y camareros.

3.2 Identificación de amenazas, impactos y riesgos

Criterios de valoración del riesgos:

Valor Cuantitativo	Valor Cualitativo	Criterio
5	Extremo	Se hace una media entre la probabilidad de que pase y los posibles daños que cause.
4	Muy Alto	Se hace una media entre la probabilidad de que pase y los posibles daños que cause.
3	Alto	Se hace una media entre la probabilidad de que pase y los posibles daños que cause.
2	Medio	Se hace una media entre la probabilidad de que pase y los posibles daños que cause.
1	Bajo	Se hace una media entre la probabilidad de que pase y los posibles daños que cause.

Amenaza	Tipos de Activos	Descripción	Riesgo
Fuego	equipos informáticos (hardware) soportes de información equipamiento auxiliar	incendios: posibilidad de que el fuego acabe con los recursos del sistema.	3
Daño por agua	equipos informáticos (hardware) soportes de información equipamiento auxiliar	inundación: posibilidad de que el agua acabe con los recursos del sistema	3
Desastres naturales	equipos informáticos (hardware) soportes de información equipamiento auxiliar	terremotos, huracanes y demás desastres que acabe con los recursos del sistema	3
Fuga de información	datos / información personal (Revelación)	revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. Degradado en una pequeña fracción baja	3
Introducción de falsa información	datos / información servicios aplicaciones (software)	introducción de falsa información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas	3

Amenaza	Tipos de Activos	Descripción	Riesgo
		específicas.	
Alteración de la información	datos / información servicios aplicaciones (software)	alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	3
Corrupción de la información	datos / información servicios aplicaciones (software)	Corrupción de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	4
Destrucción de información	datos / información servicios aplicaciones (software)	destrucción de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	4
Corte del suministro eléctrico	datos / información servicios aplicaciones (software)	indisponibilidad del uso de sistemas informáticos u otros elementos necesarios para la labor diaria	3
Condiciones inadecuadas de temperatura o humedad	datos / información servicios aplicaciones (software)	posibilidad de que los sistemas informáticos se vean afectados o su rendimiento no sea el estimado	2
Fallo de servicios de comunicaciones	datos / información servicios aplicaciones	indisponibilidad de conectarnos con la central o con el suministrador	2

Amenaza	Tipos de Activos	Descripción	Riesgo
	(software)		
Interrupción de otros servicios y suministros esenciales	datos / información servicios aplicaciones (software)	indisponibilidad de desempeñar el trabajo de forma normal	4
Desastres industriales	datos / información servicios aplicaciones (software)	posibilidad de que un desastre industrial nos deje sin fuente eléctrica y altere o perjudique al trabajo diario con los equipos de información	2
Degradación de los soportes de almacenamiento de la información	datos / información servicios aplicaciones (software)	degradado en una pequeña fracción.	2
Difusión de software dañino	datos / información servicios aplicaciones (software)	posibilidad de obtener un malware dañino o malversación da de la información empleada	3
Errores de mantenimiento / actualización de programas (software)	Aplicaciones (software)	defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	2
Errores de mantenimiento / actualización de equipos (hardware)	equipos informáticos (hardware)	defectos en los procedimientos o controles de actualización del sistema operativo que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	2

Amenaza	Tipos de Activos	Descripción	Riesgo
Caída del sistema por sobrecarga	disponibilidad / soportes de información	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	2
Pérdida de equipos	equipos informáticos (hardware) soportes de información equipamiento auxiliar	a pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. totalmente l	4
Abuso de privilegios de acceso	datos / información servicios aplicaciones (software) y equipos informáticos (hardware)	cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	4
Acceso no autorizado	datos / información servicios aplicaciones (software) equipos informáticos (hardware) soportes de información equipamiento auxiliar	el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	3
Errores de los usuarios	personal interno, información,	equivocaciones de las personas cuando usan los	

Amenaza	Tipos de Activos	Descripción	Riesgo
	servicios	servicios y datos	1
Errores del administrador	personal interno, información, servicios, aplicaciones y hardware	equivocaciones de personas con responsabilidades de instalación y operación	2
Errores de configuración	personal interno, información, servicios, aplicaciones y hardware	prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc	3
Denegación de servicio	servicios	la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	2
Robo	equipos informáticos (hardware) soportes de información equipamiento auxiliar	la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	4

Amenaza	Tipos de Activos	Descripción	Riesgo
Indisponibilidad del personal	personal interno	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica	2
Ingeniería social	personal interno	abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	4