**Test de auto-diagnóstico**



Daniel Escaño Hernández CET Ciberseguridad

# **Índice**

[**Índice**](#_u3m2w22qmzkq) **1**

[**1. Actividad 1**](#_o240jug3rzka) **2**

[**2. Actividad 2**](#_a7ofzbf0no1p) **2**

[2.1 Ejemplo de análisis](#_803z6r7fhs5) 3

[2.2 Tablas AR](#_5hpd1j75brek) 3

[2.3 Catálogo amenazas](#_c0jetenv9lw4) 4

[2.4 Activos](#_vkljvkrs60hz) 5

[2.5 Cruces Activo-Amenaza](#_jhp6gc2m0x3w) 5

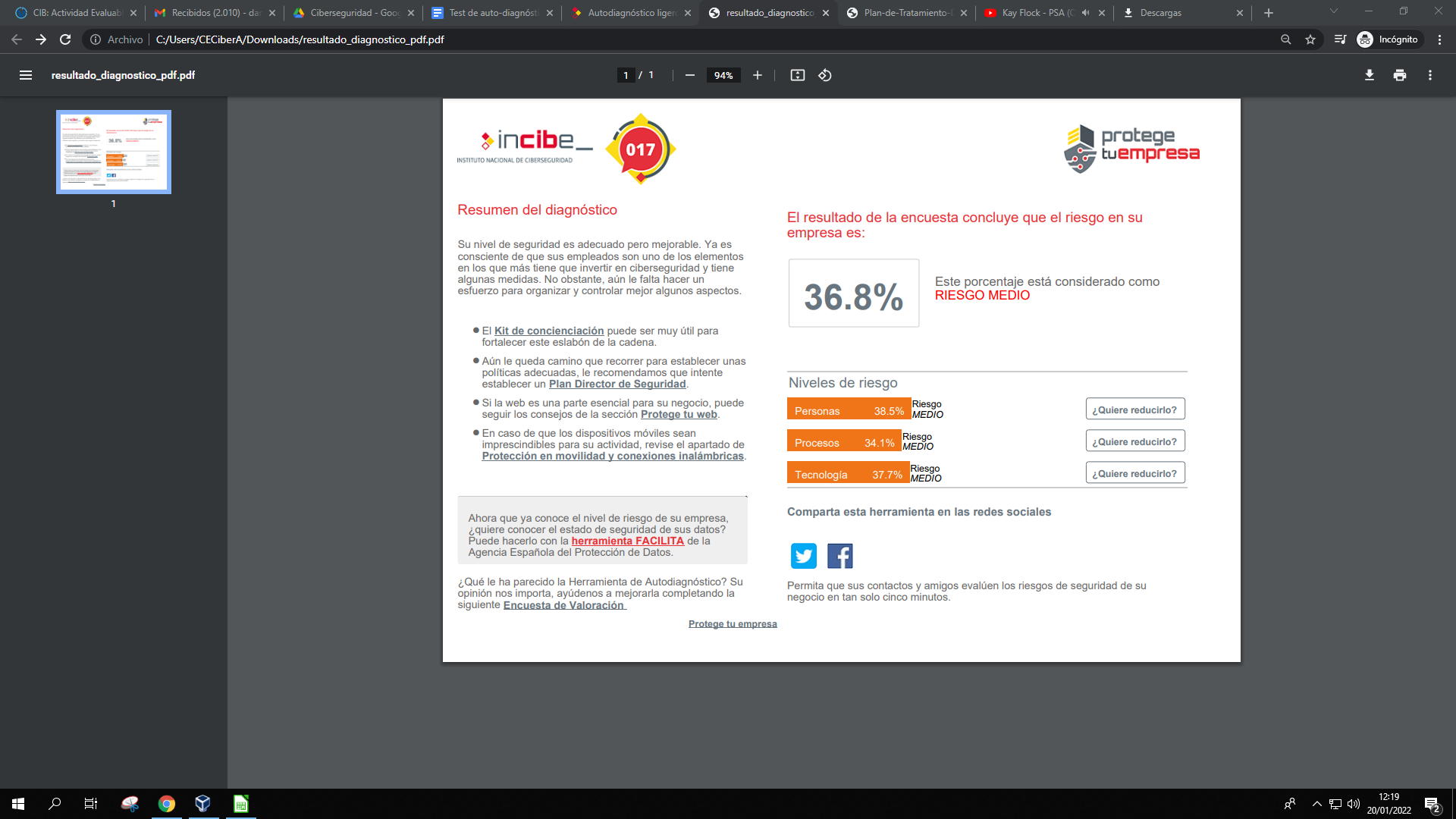
[2.6 Análisis de riesgos](#_kpsok9wn87ub) 7

[**3. Actividad 3**](#_tir7dr6rihz3) **9**

# **1. Actividad 1**

Realizar un test de auto-diagnóstico sobre los riesgos de la empresa, utilizando la herramienta que INCIBE facilita para las pymes.

Utilizar para esto los datos de una empresa ficticia.



# **2. Actividad 2**

Los alumnos deben realizar un análisis completo de riesgos, utilizando la plantilla que proporciona INCIBE. Dicha plantilla recoge las principales amenazas a considerar en el ámbito de un análisis de riesgos, basándose (con una ligera modificación) en el catálogo de amenazas de MAGERIT V3.

### **2.1 Ejemplo de análisis**

| **Análisis de riesgos** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Activo** | **Amenaza** | | | **Probabilidad** | **Impacto** | **Riesgo** |
| Servidor 01 (BBDD) | Fuga de información | | | 1 | 3 | 6 |
| Servidor 01 (BBDD) | Degradación de los soportes de almacenamiento de la información | | | 1 | 3 | 3 |
| Servidor 02 (Web) | Denegación de servicio | | | 1 | 3 | 6 |
| Servidor 02 (Web) | Corte del suministro eléctrico | | | 2 | 3 | 6 |
| Router (Internet) | Denegación de servicio | | | 1 | 2 | 2 |
| Router (Internet) | Corte del suministro eléctrico | | | 2 | 2 | 2 |
| Ordenador 01 | Fuga de información | | | 1 | 1 | 2 |
| Ordenador 01 | Denegación de servicio | | | 1 | 1 | 2 |

### **2.2 Tablas AR**

| **Tabla para estimar la probabilidad** | |
| --- | --- |
| **Valor** | **Descripción** |
| Bajo (1) | La amenaza se materializa a lo sumo una vez cada año. |
| Medio (2) | La amenaza se materializa a lo sumo una vez cada mes. |
| Alto (3) | La amenaza se materializa a lo sumo una vez cada semana |

| **Tabla para estimar el impacto** | |
| --- | --- |
| **Valor** | **Descripción** |
| Bajo (1) | El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización. |
| Medio (2) | El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización. |
| Alto (3) | El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización. |

| **Criterios de aceptación del riesgo** | |
| --- | --- |
| **Rango** | **Descripción** |
| Riesgo < 4 | La organización considera el riesgo poco reseñable. |
| Riesgo > 4 | La organización considera el riesgo reseñable y debe proceder a su tratamiento. |

### **2.3 Catálogo amenazas**

| **Amenazas** | |
| --- | --- |
| Corte del suministro eléctrico | Fuego |
| Condiciones inadecuadas de temperatura o humedad | Daños por agua |
| Fallo de servicios de comunicaciones | Desastres naturales |
| Interrupción de otros servicios y suministros esenciales | Errores de los usuarios |
| Desastres industriales | Errores del administrador |
| Alteración de la información | Errores de configuración |
| Corrupción de la información | Degradación de los soportes de almacenamiento de la información |
| Destrucción de información | Difusión de software dañino |
| Interceptación de información (escucha) | Errores de mantenimiento / actualización de programas (software) |
| Denegación de servicio | Errores de mantenimiento / actualización de equipos (hardware) |
| Robo | Caída del sistema por sobrecarga |
| Indisponibilidad del personal | Pérdida de equipos |
| Extorsión | Indisponibilidad del personal |
| Ingeniería social | Abuso de privilegios de acceso |
|  | Acceso no autorizado |

### **2.4 Activos**

|  | **Identificador** | **Activo** | **Aplicación** |
| --- | --- | --- | --- |
| Modelo C | C1 | ordenadores e incluso algún servidor (web, correo electrónico,…) | NO |
| C2 | conexión a Internet con wifi | SI |
| C3 | dispositivos móviles con datos y apps para su trabajo | NO |
| C4 | herramienta(s) comercial(es) de gestión de negocio (CRM y ERP) | SI |
| C5 | página web / tienda online y redes sociales que gestionan desde la empresa | NO |
| C6 | herramientas para empresas en la nube | SI |
| C7 | e-administración para su relación con las AAPP | NO |

### **2.5 Cruces Activo-Amenaza**

| **Amenaza \\\ Activo** | **C1** | **C2** | **C3** | **C4** | **C5** | **C6** | **C7** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Corte del suministro eléctrico | - | NO | - | SI | - | NO | - |
| Condiciones inadecuadas de temperatura o humedad | - | NO | - | SI | - | NO | - |
| Fallo de servicios de comunicaciones | - | NO | - | SI | - | NO | - |
| Interrupción de otros servicios y suministros esenciales | - | NO | - | SI | - | NO | - |
| Desastres industriales | - | NO | - | NO | - | NO | - |
| Alteración de la información | - | NO | - | SI | - | NO | - |
| Corrupción de la información | - | NO | - | SI | - | NO | - |
| Destrucción de información | - | SI | - | SI | - | SI | - |
| Interceptación de información (escucha) | - | SI | - | SI | - | SI | - |
| Denegación de servicio | - | SI | - | SI | - | SI | - |
| Robo | - | SI | - | SI | - | SI | - |
| Indisponibilidad del personal | - | SI | - | SI | - | SI | - |
| Extorsión | - | NO | - | SI | - | NO | - |
| Ingeniería social | - | NO | - | SI | - | NO | - |
| Fuego | - | SI | - | SI | - | SI | - |
| Daños por agua | - | SI | - | SI | - | SI | - |
| Desastres naturales | - | SI | - | SI | - | SI | - |
| Errores de los usuarios | - | SI | - | SI | - | SI | - |
| Errores del administrador | - | SI | - | SI | - | SI | - |
| Errores de configuración | - | SI | - | SI | - | SI | - |
| Degradación de los soportes de almacenamiento de la información | - | NO | - | SI | - | NO | - |
| Difusión de software dañino | - | SI | - | SI | - | SI | - |
| Errores de mantenimiento / actualización de programas (software) | - | SI | - | SI | - | SI | - |
| Errores de mantenimiento / actualización de equipos (hardware) | - | SI | - | SI | - | SI | - |
| Caída del sistema por sobrecarga | - | SI | - | SI | - | SI | - |
| Pérdida de equipos | - | SI | - | NO | - | SI | - |
| Indisponibilidad del personal | - | NO | - | NO | - | NO | - |
| Abuso de privilegios de acceso | - | SI | - | SI | - | SI | - |
| Acceso no autorizado | - | SI | - | SI | - | SI | - |

### **2.6 Análisis de riesgos**

| **Análisis de riesgos** | | | | |
| --- | --- | --- | --- | --- |
| **Activo** | **Amenaza** | **Probabilidad** | **Impacto** | **Riesgo** |
| **Conexión a Internet con wifi** | Destrucción de información | Bajo (1) | Medio (2) | 2 |
| Interceptación de información (escucha) | Bajo (1) | Medio (2) | 2 |
| Denegación de servicio | Bajo (1) | Medio (2) | 2 |
| Robo | Bajo (1) | Medio (2) | 2 |
| Indisponibilidad del personal | Bajo (1) | Bajo (1) | 1 |
| Fuego | Bajo (1) | Alto (3) | 1 |
| Daños por agua | Bajo (1) | Bajo (1) | 1 |
| Desastres naturales | Bajo (1) | Bajo (1) | 1 |
| Errores de los usuarios | Bajo (1) | Bajo (1) | 2 |
| Errores del administrador | Bajo (1) | Bajo (1) | 1 |
| Errores de configuración | Bajo (1) | Bajo (1) | 2 |
| Difusión de software dañino | Bajo (1) | Medio (2) | 2 |
| Errores de mantenimiento / actualización de programas (software) | Bajo (1) | Alto (3) | 3 |
| Caída del sistema por sobrecarga | Bajo (1) | Medio (2) | 1 |
| Pérdida de equipos | Medio (2) | Medio (2) | 4 |
| Abuso de privilegios de acceso | Medio (2) | Medio (2) | 4 |
| Acceso no autorizado | Medio (2) | Medio (2) | 4 |
| **Herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)** | Corte del suministro eléctrico | Bajo (1) | Alto (3) | 3 |
| Condiciones inadecuadas de temperatura o humedad | Bajo (1) | Alto (3) | 3 |
| Condiciones inadecuadas de temperatura o humedad | Bajo (1) | Alto (3) | 3 |
| Fallo de servicios de comunicaciones | Bajo (1) | Alto (3) | 3 |
| Interrupción de otros servicios y suministros esenciales | Medio (2) | Medio (2) | 4 |
| Alteración de la información | Bajo (1) | Alto (3) | 3 |
| Corrupción de la información | Bajo (1) | Alto (3) | 3 |
| Destrucción de información | Bajo (1) | Alto (3) | 3 |
| Interceptación de información (escucha) | Bajo (1) | Alto (3) | 3 |
| Denegación de servicio | Bajo (1) | Alto (3) | 3 |
| Robo | Bajo (1) | Alto (3) | 3 |
| Indisponibilidad del personal | Bajo (1) | Alto (3) | 3 |
| Extorsión | Bajo (1) | Alto (3) | 3 |
| Ingeniería social | Bajo (1) | Alto (3) | 3 |
| Fuego | Medio (2) | Alto (3) | 4 |
| Daños por agua | Bajo (1) | Alto (3) | 3 |
| Desastres naturales | Bajo (1) | Alto (3) | 3 |
| Errores de los usuarios | Bajo (1) | Alto (3) | 3 |
| Errores del administrador | Medio (2) | Medio (2) | 4 |
| Errores de configuración | Bajo (1) | Alto (3) | 3 |
| Degradación de los soportes de almacenamiento de la información | Bajo (1) | Alto (3) | 3 |
| Difusión de software dañino | Bajo (1) | Alto (3) | 3 |
| Errores de mantenimiento / actualización de programas (software) | Bajo (1) | Alto (3) | 3 |
| Caída del sistema por sobrecarga | Bajo (1) | Alto (3) | 3 |
| Abuso de privilegios de acceso | Medio (2) | Medio (2) | 4 |
| Acceso no autorizado | Bajo (1) | Alto (3) | 3 |
| **Herramientas para empresas en la nube** | Destrucción de información | Bajo (1) | Alto (3) | 3 |
| Interceptación de información (escucha) | Bajo (1) | Alto (3) | 3 |
| Denegación de servicio | Bajo (1) | Alto (3) | 3 |
| Robo | Bajo (1) | Alto (3) | 3 |
| Indisponibilidad del personal | Bajo (1) | Alto (3) | 3 |
| Fuego | Bajo (1) | Alto (3) | 3 |
| Daños por agua | Bajo (1) | Alto (3) | 3 |
| Desastres naturales | Bajo (1) | Alto (3) | 3 |
| Errores de los usuarios | Bajo (1) | Alto (3) | 3 |
| Errores del administrador | Bajo (1) | Alto (3) | 3 |
| Errores de configuración | Bajo (1) | Alto (3) | 3 |
| Difusión de software dañino | Bajo (1) | Alto (3) | 3 |
| Errores de mantenimiento / actualización de programas (software) | Bajo (1) | Alto (3) | 3 |
| Errores de mantenimiento / actualización de equipos (hardware) | Bajo (1) | Alto (3) | 3 |
| Caída del sistema por sobrecarga | Bajo (1) | Alto (3) | 3 |
| Pérdida de equipos | Bajo (1) | Alto (3) | 3 |
| Abuso de privilegios de acceso | Bajo (1) | Alto (3) | 3 |
| Acceso no autorizado | Bajo (1) | Alto (3) | 3 |

# **3. Actividad 3**

Diseñar un mapa conceptual sobre la ISO 31000.

