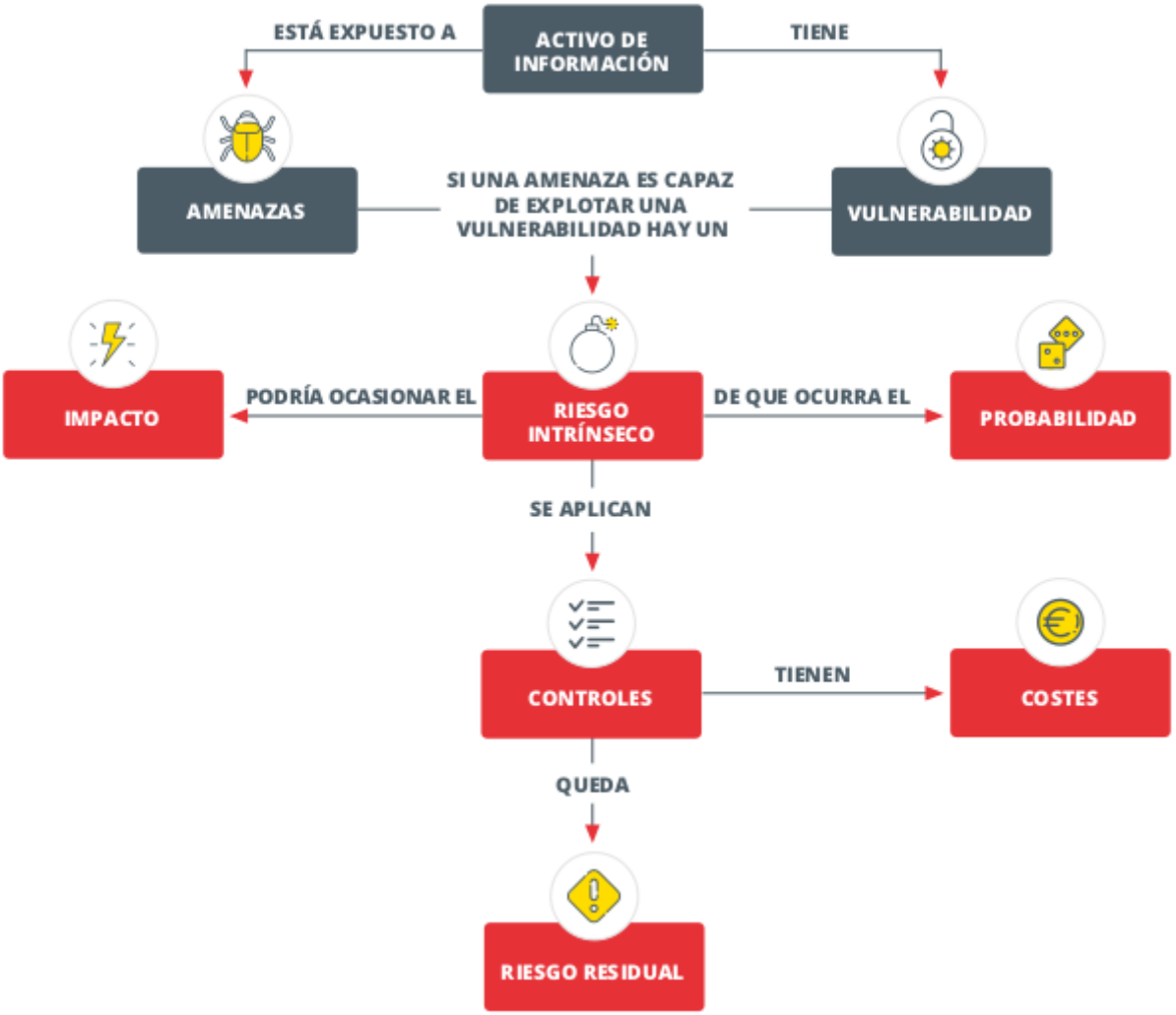

I+D: Análisis de riesgos

Grupo 4: Ignacio, Daniel, Álvaro, Jesús y María
Incidentes de seguridad

ÍNDICE

0. Introducción

Grupo e integrantes: Grupo 4. Ignacio, Daniel, Álvaro, Jesús y María.

Contexto de la empresa: La empresa trata de que los clientes contacten con la empresa para que realicen trabajos. Dicha empresa está formada por 150 empleados distribuidos en dos sedes con diferentes departamentos. A causa de la evolución de la empresa y de las tecnologías, la empresa decidió desarrollar un plan estratégico de transformación digital, para extenderse y realizar la mayoría de sus trabajo a través de Internet, apoyándose en la página web.

Objetivo de la empresa: La empresa creó un plan de transformación digital de sus servicios, a causa de la digitalización de la empresa. Por tanto precisa de realizar un plan para abordar los posibles riesgos y realizar una gestión planificada de las actuaciones en materia de ciberseguridad.

Departamentos: Facturación y ventas, compras, comunicación y RRSS, TIC, RRHH, Delivery, Mantenimiento, Legal y un consejo de administración.

Instalaciones/Sedes: Dos sedes, una en un edificio donde está la sede principal y otra en la segunda planta de otro edificio que alberga otras empresas.

Servicios TIC:

- Gestión de copias de seguridad almacenadas en la sede principal.
- Gestión de antivirus controlado por la empresa subcontratada.
- Cumplimiento de la RGPD a través de la contratación de una consultoría
- Gestión de firewall con una zona privada y una zona pública.
- Segmentación de la red por departamentos
- Página web alojada en un servidor externo, seguridad mantenida por el servicio en el cual está alojado.

1. Alcance del análisis

El área que vamos a analizar es el departamento de TIC, ya que el mal funcionamiento o gestión de éste, puede afectar a las actividades de la empresa a nivel comercial y a la operativa interna y externa, así como, el tratamiento de la información de clientes, personal y servicios.

La estrategia que seguirá la empresa es abordar los posibles riesgos y realizar una gestión planificada de las actuaciones en materia de ciberseguridad.

2. Identificación de los activos

Expondremos aquellos activos más importantes que guardan relación con el departamento/proceso objeto del estudio (Dpto. TIC).

Activos	Descripción
Puestos de trabajo	PC, impresoras y teléfonos.
Dispositivos móviles	Portátiles, móviles y tabletas.
Sistemas de almacenamiento	Discos duros y pendrive.
Servidores de la empresa	Serv. correo, archivos y aplicaciones.
Conexiones a internet	Routers y Wifi.
Datos e información de la empresa	Datos de clientes, proveedores, funcionamiento y gestión de la empresa
Propiedad intelectual	Creaciones de la empresa.
Procesos en aplicaciones	procesos internos en aplicaciones como CRM y ERP
Datos e información en la nube o servidor	Datos e información almacenados en la nube o en los servidores.
Aplicaciones en la nube	Aplicaciones almacenadas en servidores en la nube.

3. Amenazas que pueden afectar a los activos

Amenazas
Daños por fuego, agua o desastres naturales.
Respecto a la información: fuga, destrucción, alteración, corrupción e intercepción.
Errores de usuario, administrador y configuración.
Fallo de suministro eléctrico, comunicación, temperatura y servicios esenciales
Errores de mantenimiento de software y hardware.
Acceso no autorizado por abuso de privilegios.
Degradación de los soportes de almacenamiento .
Difusión de malware.
Robo, extorsión e ingeniería social.
Denegación de los servicios.

4. Identificar vulnerabilidades y salvaguardas

4.1 Identificación de salvaguardas (Medidas y controles de seguridad)

- Instalar y configurar un firewall que proteja la red de la empresa.
- Instalar equipos de protección contra sobrecargas (SAI) y cortes de corriente.
- Crear una política de backup automatizado, probada, actualizada y documentada con una copia de respaldo.
- Crea una política de tratamiento y destrucción de los datos y documentos que genere la empresa.
- Diseñar una política de administración de cuentas, gestión y protección de contraseñas.
- Contratar un seguro para los móviles, tablets, portátiles de la empresa en caso de pérdida, extravío o rotura.
- Contratar a un servicio externo en la segunda sede que se encargue del control de acceso a la empresa.

- Crear una política de control de accesos físicos para establecer quién, cómo y cuándo y dónde pueden acceder a los activos de información de la empresa y registrar dichos accesos, así como de acceso remoto.
- Crear y desplegar un plan de concienciación en materia de seguridad y así como una política de comunicación para mantener informada a la dirección y a la plantilla.

4.2 Vulnerabilidades/Debilidades

- No disponer de un firewall.
- Sistema automatizado de backups y encriptación de discos.
- No existe una política de destrucción de datos, informes y soportes.
- Sistema de administración de cuentas de usuario.
- En cuanto a los dispositivos móviles, no disponer de un plan B en caso de que se estropeen, extravíen o pierdan.
- Control de accesos con identificaciones.
- No tener un sistema de control de acceso virtual, monitorizado y actualizado para el uso remoto de nuestros sistemas por parte de los empleados.
- No tener una política de concienciación de nuestros trabajadores en seguridad de la información.
- No disponer de una política de comunicación.
- Equipos vulnerables a cambios de voltaje/sobrecargas.

5. Evaluación y cálculo del riesgo

A continuación expondremos las amenazas de mayor umbral que afectan a los activos, las demás amenazas, expuestas anteriormente, serán aceptadas por la empresa asumiendo sus consecuencias.

Para cada activo-amenaza, se expondrán las amenazas superiores de 4, por debajo de 4 aceptaremos el riesgo. Dividiremos la tabla a continuación en dos columnas, la amenaza y los activos a los que afecta dicha amenaza.

Amenaza	Activos
Fuga de información	Ordenadores/Servidores, Página web/Tienda online y RRSS, Herramientas en la nube, Herramientas para la administración online
Alteración de la información	Ordenadores/Servidores, Dispositivos moviles, Página Web/Tienda online y RRSS, Herramientas en la nube, Herramientas para la administración online
Corrupción de la información	Ordenadores/Servidores, Dispositivos moviles, Página Web/Tienda online y RRSS, Herramientas en la nube, Herramientas para la administración online
Destrucción de la información	Ordenadores/Servidores, Dispositivos moviles, Herramientas comerciales, Página Web/Tienda online y RRSS, Herramientas en la nube, Herramientas para la administración online
Difusión de software dañino	Ordenadores/Servidores, Dispositivos moviles, Página Web/Tienda online y RRSS, Herramientas en la nube
Errores de mantenimiento o actualización de software y hardware	Ordenadores/Servidores
Denegación de servicio	Página web/Tienda online y RRSS, Herramientas en la nube
Caída del sistema por sobrecarga	Página web/Tienda online y RRSS

Amenaza	Activos
Abuso de privilegios de acceso	Ordenadores/Servidores, Conexión a Internet con wifi, Dispositivos móviles, Herramientas comerciales, Página web/Tienda online y RRSS, Herramientas en la nube, Herramientas para la administración online
Acceso no autorizado	Ordenadores/Servidores, Conexión a Internet con wifi, Herramientas para la administración online
Ingeniería social	Ordenadores/Servidores, Dispositivos móviles, Página web/Tienda online y RRSS, Herramientas en la nube
Intercepción de la información	Ordenadores/Servidores, Conexión a Internet con wifi, Dispositivos móviles, Herramientas comerciales, Herramientas en la nube, Herramientas para la administración online
Robo	Dispositivos móviles, Página web/Tienda online y RRSS
Extorsión	Ordenadores/Servidores, Dispositivos móviles
Errores de los usuarios, administrador o configuración	Dispositivos móviles, Herramientas comerciales

6. Medidas complementarias que permitan materializar la protección de los activos.

Tomar una estrategia para tratar el riesgo y obtener riesgo residual tras aplicar estrategia. Iniciativas para implantar controles o salvaguardas.

- Cifrado de la información confidencial corporativa.
- Instalación, configuración y actualización de los cortafuegos.
- Mantener actualizadas las aplicaciones de nuestros sistemas.
- Crear copias de seguridad, verificando su integridad.
- Crear una política de tratamiento y destrucción de los datos y documentos que genere la empresa.
- Crear una política de descarga de archivos para los usuarios con correo electrónico.
- Que sólo los usuarios con rol administrador puedan descargar programas.
- Mantener actualizado tanto el Hardware como el software de la empresa.
- Ubicar el servidor en una DMZ para que el atacante no tenga acceso a la red.
- Usar un sistema de detección y prevención de ataques (IDS/IPS)
- Aumentar el ancho de banda.
- Implementar redundancia del servidor y balanceo de carga.
- Usar un cortafuegos de aplicación (soluciones basadas en la nube).
- Crear una política de privilegios por la que los usuarios solo tendrán los permisos necesarios para el desempeño de sus funciones.
- Crear políticas de autenticación seguras.
- Restringir el acceso a la red mediante filtrado MAC.
- Cifrar la comunicación en la red.
- Dar formación sobre seguridad a los trabajadores.
- Tener herramientas para monitorizar los sistemas.
- No pagar frente a extorsiones y robos y mantener copias de seguridad actualizadas para poder recuperar la información sustraída.

7. Conclusión

En este análisis de riesgos, se ha hablado de muchos riesgos y su posible prevención y, como se ha visto anteriormente, la mayor parte de los riesgos se pueden prevenir. Para ello hacen falta medidas técnicas, humanas y organizacionales. Es decir, con revisiones técnicas, educación respecto a los riesgos en materia de seguridad, su prevención y las medidas que imponga la organización o empresa, conseguiremos reducir notablemente los accidentes.

Después de realizar el análisis al departamento de TIC, y del cual dependen el resto de departamentos, se ha localizado una serie de vulnerabilidades que afectan a la seguridad de la red, por ello en el documento expuesto, se muestra una serie de pautas a implementar para la correcta securización de la empresa y la reducción de las amenazas intentando llevar estas al mínimo para que así tanto la actividad de la empresa como los datos que esta maneja, se encuentren correctamente protegidos.

8. Bibliografía/Webgrafía

- www.incibe.es
- https://ayudaleyprotecciondatos.es/2020/10/30/plan-director-de-seguridad/
- https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf
- https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguridad-en-internet.pdf
- https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad