Gestión de riesgos de seguridad de la información

Autores: Valentina Vispo y Marcelo Raidán.

¿Qué nivel de madurez le asignaría a la organización?

Para poder definir en qué nivel se encuentra este caso de estudio, primero debemos comprender qué niveles existen y cuál es la descripción de cada nivel. El modelo de madurez CMM nos da una clasificación clara, consta de 5 niveles:

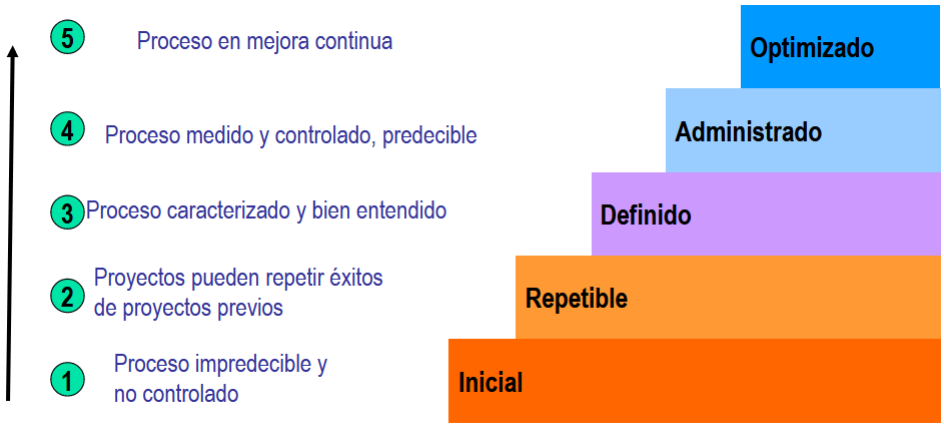
1 - **Inicial**. Las organizaciones en este nivel no disponen de un ambiente estable para el desarrollo y mantenimiento de software. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado de los proyectos es impredecible.

2 - **Repetible**. En este nivel las Organizaciones disponen de unas prácticas institucionalizadas de gestión de proyectos, existen unas métricas básicas y un razonable seguimiento de la calidad. La relación con subcontratistas y clientes está gestionada sistemáticamente.

3 - **Definido**. Además de una buena gestión de proyectos, a este nivel las organizaciones disponen de correctos procedimientos de coordinación entre grupos, formación del personal, técnicas de ingeniería más detallada y un nivel más avanzado de métricas en los procesos. Se implementan técnicas de revisión por pares (peer reviews).

4 - **Gestionado**. Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad.

5 - **Optimizado**. La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.



Del análisis del caso de estudio, la organización posee un nivel **INICIAL**.

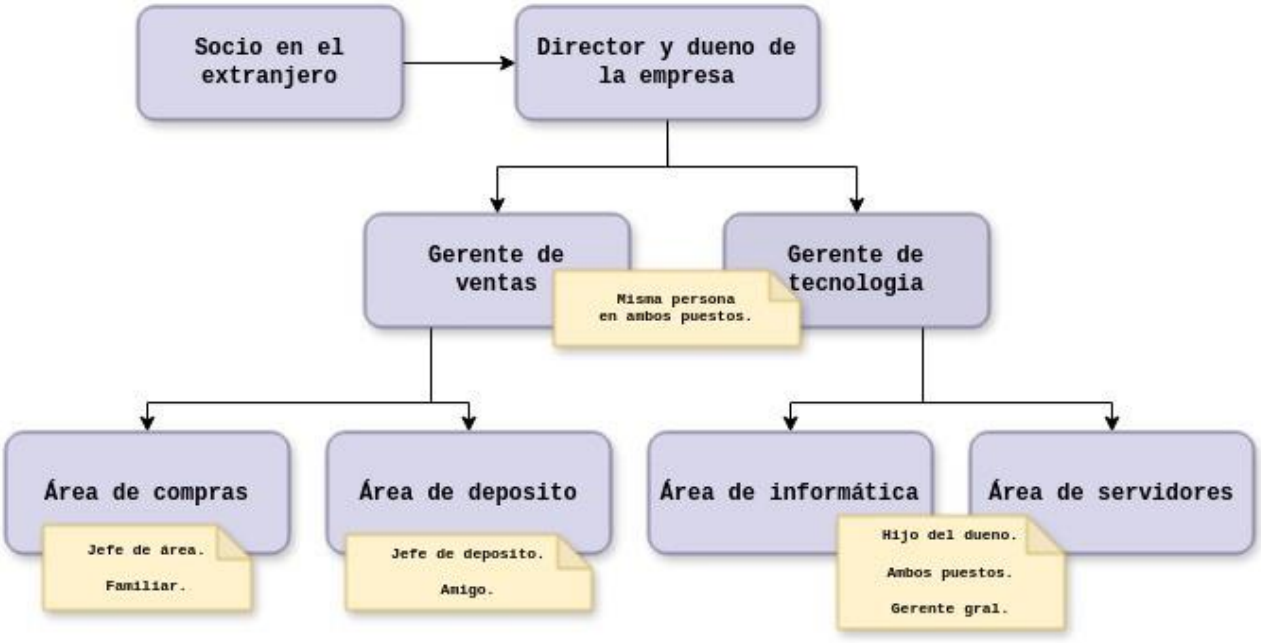
a) Se propone para iniciar un ciclo de mejoras continuas en toda la empresa, comenzar por los procesos internos para poder elevar la gestión de los proyectos aumentando y haciendo aumentar la calidad en el proceso utilizando métricas y mejores prácticas. Ingresando en un ciclo de Deming de mejora continua.
Mejorar la administración con los subcontratistas y clientes. Luego analizar el avance para poder subir un escalón en el modelo CMM.
El nivel 2 Repetible. En la próxima evaluación anual de los procesos internos se podrá, con la experiencia, comenzar a madurar los procesos y por ende, comenzar con la madurez de la organización.

2) Organización ficticia

"**Auto Park-T**" es una tienda que se dedica a la venta de autopartes. Una empresa familiar, pequeña e inmadura que está en proceso de expansión dado que uno de sus socios, un familiar que se encuentra en el extranjero y que fabrica autopartes de buena calidad, les permiten ser los únicos en el país que traen dichas autopartes importadas a buen precio. Esta organización empresarial, ha crecido en un entorno familiar en donde el dueño (director), es el fundador y su Hijo, con los conocimientos básicos y de forma autodidacta ha armado la infraestructura tecnológica que le ha permitido aumentar las ventas incluso durante la pandemia del 2020.

Debido a una serie de incidentes informáticos que por culpa de su infraestructura obsoleta y mal configurada lo han perjudicado en las ventas, su padre y su socio en el extranjero le solicitaron al hijo, contratar un CISO para reestructurar e invertir en seguridad, como así también armar un plan para profesionalizar a los familiares y amigos que trabajan en dicha empresa, contratando a una consultora que reorganice y capacite las áreas y poder elevar el nivel de madurez empresarial. Para esto el socio en el extranjero está dispuesto a invertir USD 100.000 en la reestructuración.

Estructura organizacional actual



Identificar los activos de la organización

Al ser una empresa familiar, no tienen muchos activos.

Clasificación por tipo de información

DATOS	SISTEMAS	PERSONAL
[D_int_aplicación] Datos Aplicación	[Media_electronic_disk_externo] Disco externo	[P_ui_gerentes] Ejecutivos
[D_backup_aplicacion] Respaldos aplicación.	[HW_pc_et] Estación de trabajo	[P_adm_tecnologia] Administradores de TI
[D_int_bases] Base de datos	[HW_mobie_notebook] Notebook	[P_ui_empleados] Usuarios de los sistemas
[D_password_servidor] Claves servidor i	[COM_wifi_router] Router WiFi	[P_adm_plataforma] Administradores plataforma
[D_int_mail] correos electrónicos	[HW_host_servidor] Servidor 1	[P_ui_wifi] Usuarios de wifi
[D_files_compartidos] Directorios compartidos	[HW_host_servidor] Servidor 2	[P_adm_aplicación] Administradores aplicación
[D_int_aplicación] Datos de la plataforma	[HW_host_servidor] Servidor 3	-
[D_source_aplicacion] Programas fuentes	-	-
[D_files_archivos] Sistema de archivos	-	-

Elegir las dimensiones de la clasificación

(**Integridad,**
disponibilidad,
confidencialidad)

Clasificar las informaciones

Impacto / Magnitud de Daño:
Leve=1
Menor=2
Moderado=3
Alto=4
Extremo=5

	I	D	C	
[D_int_aplicación] Datos Aplicación	4	3	4	4
[D_backup_aplicacion] Respaldos aplicación.	3	5	4	5
[D_int_bases] Base de datos	4	3	3	4
[D_password_servidor] Claves servidor i	4	5	5	5
[D_int_mail] correos electronicos	3	2	3	3
[D_files_compartidos] Directorios compartidos	2	3	3	3
[D_int_aplicación] Datos de la plataforma	1	2	1	2
[D_source_aplicacion] Programas fuentes	2	1	3	3
[D_files_archivos] Sistema de archivos	3	4	3	4

	I	D	C	
[Media_electronic_disk_externo] Disco externo	4	5	5	5
[HW_pc_et] Estación de trabajo	2	3	5	5
[HW_mobie_notebook] Notebook	1	3	3	3
[COM_wifi_router] Router WiFi	3	3	3	3
[HW_host_servidor] Servidor 1	3	5	5	5
[HW_host_servidor] Servidor 2	4	5	5	5
[HW_host_servidor] Servidor 3	4	5	5	5

	I	D	C	
[P_ui_gerentes] Ejecutivos	3	3	3	3
[P_adm_tecnologia] Administradores de TI	3	3	5	5
[P_ui_empleados] Usuarios de los sistemas	3	4	5	5
[P_adm_plataforma] Administradores plataforma	4	4	5	5
[P_ui_wifi] Usuarios de wifi	1	3	3	3
[P_adm_aplicación] Administradores aplicación	4	4	5	5

Cuáles son los activos mínimos que se desprenden de la descripción de los incidentes.

DATOS E INFORMACION
A1 - datos de la aplicacion
B1 - backup
BD - base de datos
C1 - Contraseñas
S2 - Servicio de Correo elec.
DC - directorios compartidos
PL - datos de plataforma
CF - codigo fuente
DS - datos sistema de archiv.

SISTEMAS Y EQUIPOS
N1 - Notebook dueño
WF - Wifi corporativo
S1 - Servidor general
SW - Servidor WEB
DE - disco externo
ET - estacion de trabajo
CE - Correo Electronico

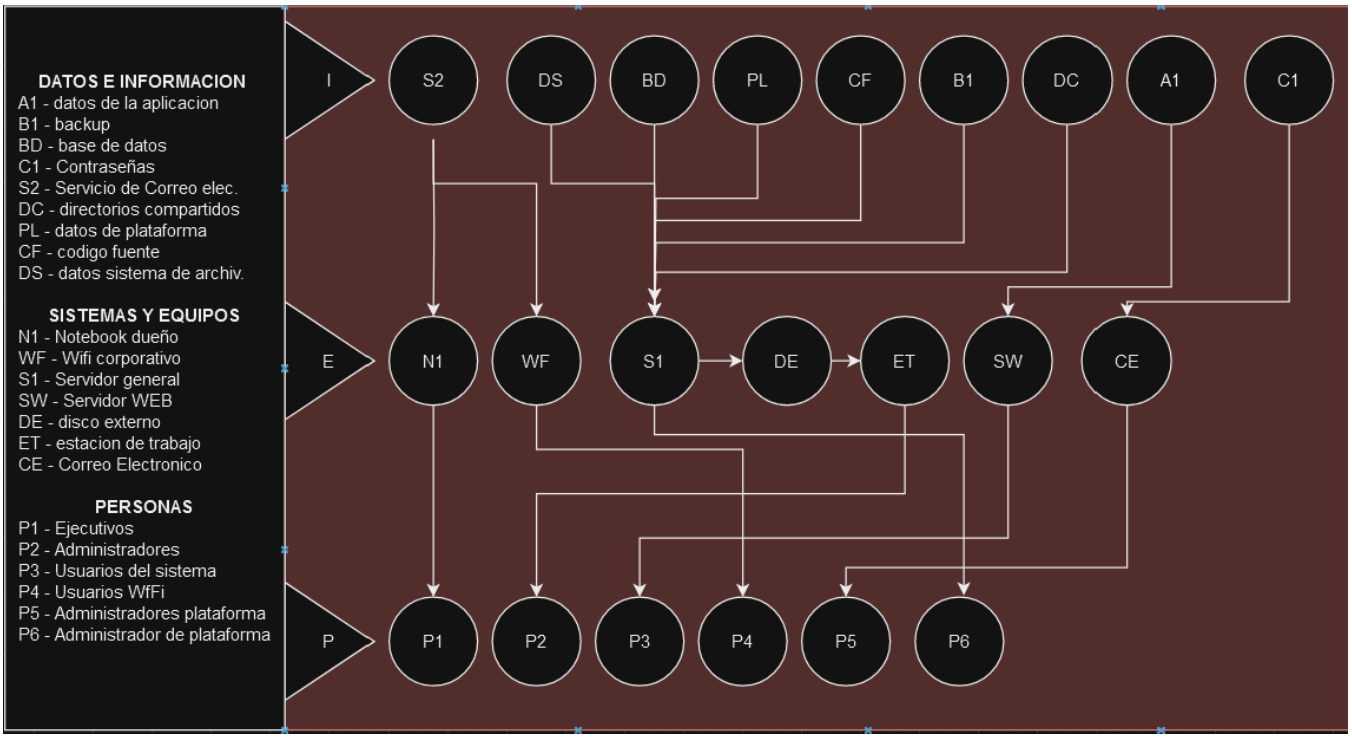
PERSONAS
P1 - Ejecutivos
P2 - Administradores
P3 - Usuarios del sistema
P4 - Usuarios WfFi
P5 - Administradores plataforma
P6 - Desarrolladores web

Inventario con clasificación, traducción a Magerit

Clasificación nuestra	Clasificación con Magerit
A1 – Datos de la aplicación	[D_int_aplicación] Datos Aplicación
B1 - Backup	[D_backup_aplicacion] Respaldos aplicación.
BD – Base de datos	[D_int_bases] Base de datos
C1 – Contraseñas	[D_password_servidor] Claves servidor i
S2 – Servicio de correo electro…	[D_int_mail] correos electronicos
DC – Directorios compartidos	[D_files_compartidos] Directorios compartidos
PL – Datos de plataforma	[D_int_aplicación] Datos de la plataforma
CF – Codigo fuente	[D_source_aplicacion] Programas fuentes
DS – Datos sistemas de archivos	[D_files_archivos] Sistema de archivos

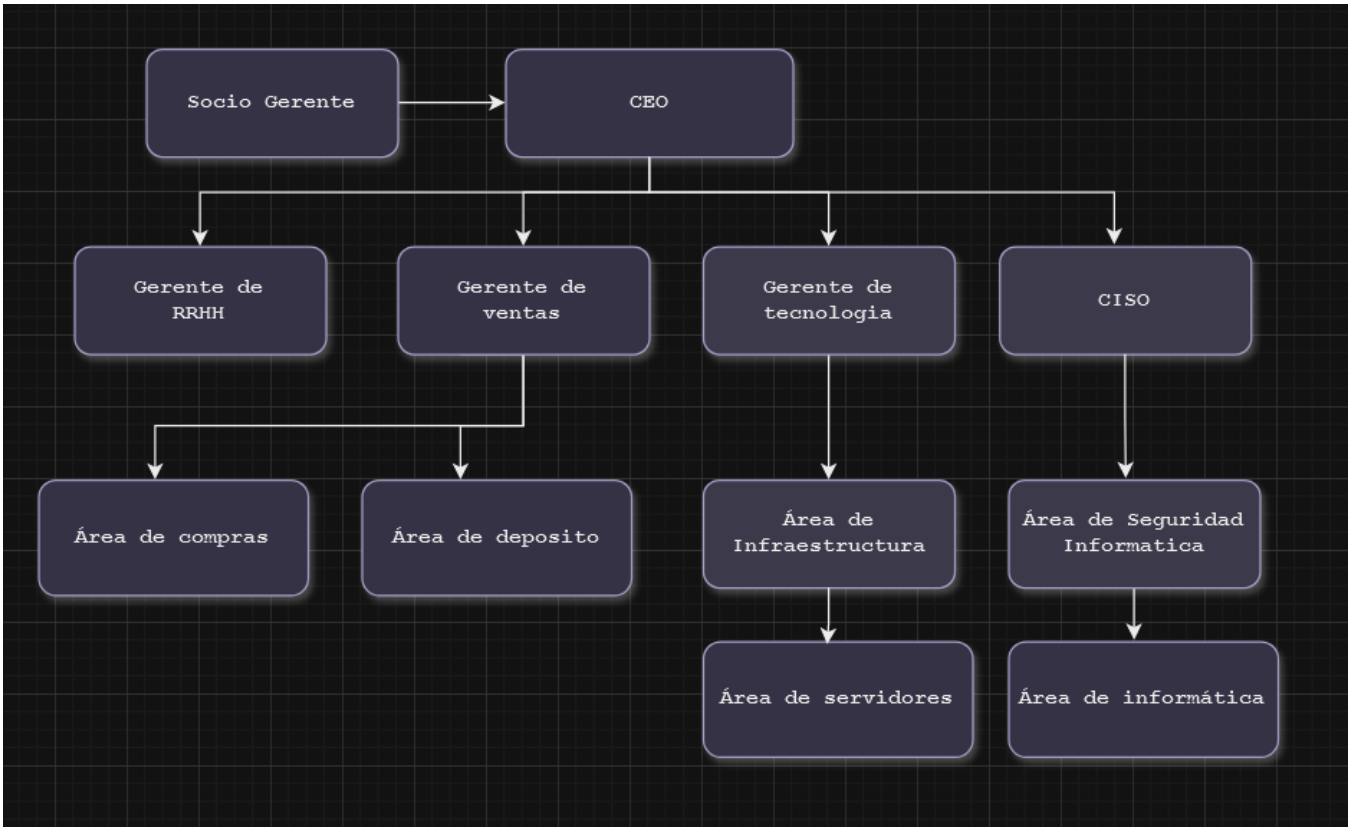
Clasificación nuestra	Clasificación con Magerit
N1 – Notebook dueño	[HW_mobie_notebook] Notebook
WF – Wifi corporativo	[COM_wifi_router] Router WiFi
S1 – Servidor general	[HW_host_servidor] Servidor 1
SW – Servidor Web	[HW_host_servidor] Servidor 2
DE – Disco externo	[Media_electronic_disk_externo] Disco externo
ET – Estacion de trabajo	[HW_pc_et] Estación de trabajo
CE – Correo electrónico	[HW_host_servidor] Servidor 3
P1 – Ejecutivos	[P_ui_gerentes] Ejecutivos
P2 – Administradores	[P_adm_tecnologia] Administradores de TI
P3 – Usuarios del sistema	[P_ui_empleados] Usuarios de los sistemas
P4 – Usuarios Wifi	[P_ui_wifi] Usuarios de wifi
P5 – Administradores de plataforma	[P_adm_plataforma] Administradores plataforma
P6 – Desarrolladores web	[P_adm_aplicación] Administradores aplicación

Árbol de activos



4) Estructura organizacional para la seguridad de la información

Nuestra propuesta organizacional es la siguiente:



El rol de CISO se encuentra debajo del CEO, pero a la misma altura que los gerentes. Lidera de manera directa al Área de Seguridad Informática, pero trabaja a la par con otras áreas para mejorar la calidad de la seguridad empresarial.

5) Matriz de análisis de riesgos

Probabilidad de Vulnerabilidad [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]
Impacto [1=Leve, 2=Menor, 3=Moderado, 4=Alto, 5=Extremo]

Datos

Matriz de Análisis de Riesgo	Clasificación				abilidad [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]															
									Sucesos de origen físico							Amenazas internas							
Datos e Información	Integridad	Disponibilidad	Confidencialidad	Magnitud de Daño: [Leve=1 Menor=2 Moderado=3 Alto=4 Extremo=5]	malware	ofensa	Extorsión	Fraude / Estafa	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Ausencia de documentación
					3	2	3	2	3	2	2	1	3	2	3	4	3	4	3	3	3	3	4
[D_int_aplicación] Datos Aplicación	x	x	x	4	12	8	12	8	12	8	8	4	12	8	12	16	12	16	12	12	12	12	16
[D_backup_aplicacion] Respaldos apli	x	x	x	5	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[D_int_bases] Base de datos	x	x	x	4	12	8	12	8	12	8	8	4	12	8	12	16	12	16	12	12	12	12	16
[D_password_servidor] Claves servido	x	x	x	5	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[D_int_mail] correos electronicos	x	x	x	3	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[D_files_compartidos] Directorios con	x	x	x	3	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[D_int_aplicación] Datos de la plataforr	x	x	x	2	6	4	6	4	6	4	4	2	6	4	6	8	6	8	6	6	6	6	8
[D_source_aplicacion] Programas fuer	x	x	x	3	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[D_files_archivos] Sistema de archivos	x	x	x	4	12	8	12	8	12	8	8	4	12	8	12	16	12	16	12	12	12	12	16

Sistemas

Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Vulnerabilidad [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																			
					Ciber amenazas							Sucesos de origen físico							Amenazas internas							
Sistemas e Infraestructura	Integridad	Disponibilidad	Confidencialidad	Magnitud de Daño: [Leve=1 Menor=2 Moderado=3 Alto=4 Extremo=5]	Ransomware	Phishing	Fuga de credenciales	malware	ofensa	Extorsión	Fraude / Estafa	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Ausencia de documentación
					4	3	4	3	2	3	2	3	2	2	1	3	2	3	4	3	4	3	3	3	3	4
[Media_electronic_disk_externo] Disco ext	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[HW_pc_et] Estación de trabajo	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[HW_mobile_notebook] Notebook	x	x	x	3	12	9	12	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[COM_wifi_router] Router WiFi	x	x	x	3	12	9	12	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[HW_host_servidor] Servidor 1	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[HW_host_servidor] Servidor 2	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[HW_host_servidor] Servidor 3	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20

Personas

Matriz de Análisis de Riesgo					Probabilidad de Vulnerabilidad [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																						
Personal	Clasificación			Magnitud de Daño: [Leve=1 Menor=2 Moderado=3 Alto=4 Extremo=5]	Ciber amenazas							Sucesos de origen físico							Amenazas internas							
	Integridad	Disponibilidad	Confidencialidad		Ransomware	phishing	Fuga de credenciales	malware	ofensa	Extorsión	Fraude / Estafa	Incendio	Inundación / destave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software 'pirateado'	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Ausencia de documentación
					4	3	4	3	2	3	2	3	2	2	1	3	2	3	4	3	4	3	3	3	3	4
[P_ui_gerentes] Ejecutivos	x	x	x	3	12	9	12	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[P_adm_tecnologia] Administradores de T	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[P_ui_empleados] Usuarios de los sistema	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[P_adm_plataforma] Administradores plat	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20
[P_ui_wifi] Usuarios de wifi	x	x	x	3	12	9	12	9	6	9	6	9	6	6	3	9	6	9	12	9	12	9	9	9	9	12
[P_adm_aplicación] Administradores aplic	x	x	x	5	20	15	20	15	10	15	10	15	10	10	5	15	10	15	20	15	20	15	15	15	15	20

6) Medidas de remediación o contramedidas

La gestión de los riesgos es nuclear al gobierno de las organizaciones. En particular, los riesgos que tienen su origen en el uso de tecnologías de la información deben trasladarse a los órganos de gobierno y contextualizarse en la misión de la organización.

El conocimiento de los riesgos permite calibrar la confianza en que los sistemas desempeñarán su función como la Dirección espera, habilitando un marco equilibrado de Gobierno, Gestión de Riesgos y Cumplimiento (GRC), tres áreas que deben estar integradas y alineadas para evitar conflictos, duplicación de actividades y zonas de nadie.

Control de acceso

Una política de control de acceso es un conjunto de condiciones que, una vez evaluadas, determinan las decisiones de acceso o rechazo.

Las condiciones son una combinación de atributos, obligaciones, políticas de autenticación y un perfil de riesgo.

Gestión de respaldos

1. Realizar backups con frecuencia.
2. Mantener las copias de seguridad cifradas.
3. Contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar la pérdida generalizada de datos.
4. Elaborar un plan detallado que contemple los sistemas, aplicaciones y datos que se integrarán con la solución de respaldo y que ayudarán a mejorar la eficiencia, la organización y, en última instancia, la productividad.
5. Tener en cuenta que el respaldo no es únicamente tener copias de datos, sino que su verdadero objetivo es la recuperación ante desastres. Si las copias de seguridad se realizan con regularidad, se reducirán los tiempos de recuperación en caso de un incidente, ya que será más fácil localizar exactamente qué copia de seguridad tratará el incidente de pérdida de datos.

Política y procedimiento de disaster recovery

Todo componente del sistema productivo debe estar contemplado en un proceso de recuperación que cubre los datos, el hardware y software crítico. El mismo debe probarse cada un año y realizar un informe del proceso.

Software antivirus, anti-spam y anti-malware

Dado que podemos sufrir un intento de vulneración, todos los sistemas deben contar con antivirus de ámbito empresarial, el cuál debe estar actualizado al día y debe permitir configurar alertas. Aquellos sistemas que no puedan, por razones de confidencialidad o técnicas, hacer uso de este antivirus, deberán tener mayores controles y restricciones para el acceso.

Capacitación de personal y directivos

Capacitaciones continuas correspondientes a los riesgos de seguridad de la información, algunos ejemplos de estos son:

1. Phishing
2. Confidencialidad
3. Canales seguros de comunicación
4. Contraseñas y credenciales

Gestión de las estaciones de trabajo

Dado que un mal manejo de las estaciones de trabajo posibilita un vector de ataque, se deben definir reglas claras para realizar la labor en el día a día. Algunas políticas o reglas que podemos mencionar son las siguientes:

1. No se permite el uso de notebooks personales para trabajar.
2. Todas las notebooks del trabajo poseen sistemas operativos actualizados, con antivirus y firewall activo.
3. No se permite compartir notebook de trabajo con los compañeros.
4. Cuando uno se levanta de la estación de trabajo, debe cerrar las sesiones activas de consola y bloquear la notebook.
5. Las notebooks de trabajo deben tener contraseña fuerte.
6. Las notebooks de trabajo deben tener sus discos cifrados.

Auto escalado de servicios

Para que el servicio que prestamos no este caído debemos tener la posibilidad de escalar de manera horizontal y vertical. Una manera de realizar esto, es con la contratación de servicios Cloud (AWS, Azure, GCP, etc.) ya que dan soluciones a estos problemas de manera predeterminada, pero para ello se deberá migrar la infraestructura a este nuevo entorno. Si no, se puede optar por utilizar herramientas para el entorno físico, y comprar más infraestructura, que puede estar siendo utilizada o no.

Cambiar la configuración a una segura (no predeterminada)

Todo sistema, debe realizar una configuración inicial previa a su uso. Es decir, que cada sistema a estrenar debe configurarse distinto a la configuración por defecto.

La configuración debe denegar siempre toda conexión, acceso o respuesta a los agentes que no estén especificados como “permitido”. A su vez, si el sistema posee contraseñas, credenciales o cualquier método

de autenticación, se debe realizar una nueva clave, credenciales, etc.; con el fin de que ésta sea diferente y cumpla con las políticas y normas establecidas por la organización.

Separación de funciones

Se requiere de personal idóneo para cada tarea, con responsabilidades claras y correspondientes a su área al igual que se debe establecer los accesos y permisos mínimos y necesarios para cubrir sus tareas diarias.

Video vigilancia

Agregar cámaras de seguridad en la entrada de los servidores físicos: de esta manera se puede corroborar no solo con el historial de los controles establecidos para ingreso, sino que se cuenta con evidencia de video. Estas grabaciones deben realizarse con backups offline, que únicamente el dueño de la empresa cuente con acceso al mismo.

Política y control de contraseñas

Los colaboradores deben ser comprender el riesgo que supone tener contraseñas débiles, o utilizar la misma contraseña fuerte en múltiples accesos. Debe implementarse políticas y controles respecto a la creación y actualización de las mismas, estableciendo configuraciones predeterminadas y obligatorias en todos los accesos que sea posible.

Monitoreo

Para detectar una eventual anomalía o intrusión en los sistemas, se deben tener controles de registros y logs. Los mismos deben ser accesibles para auditar en cualquier momento.

Separar servicios

Se deben aislar, segmentar y separar los servicios unos de otros. En el caso de que un servicio necesite conexión con otro, aplicar el concepto Zero Trust para las conexiones.

¿Por qué realizar esta separación si agrega “pasos extras”?

Porque si un sistema (servicio) se ve infectado por otro, en el caso de que éstos nos estuvieran segmentados, la propagación de la infección sería mucho más fácil, rápida y efectiva. Con este aislamiento, posibilitamos el tiempo de respuesta y, en el mejor de los casos, aumentamos el tiempo en el que todo el sistema estaría comprometido.

El orden de preferencia para la implementación de las contramedidas, es deseable que se realicen dentro de un marco de proceso normativo y mediante un proyecto, comenzando por aquellos riesgos que en la matriz de riesgos están en critico. (Rojo).

Ya que el efecto deseado en el riesgo es que este no se concrete.

Bibliografía y referencias

Casos de Estudio - https://1drv.ms/w/s!AgPblH2kU90WiM1QkDx3Sh-4zPGNgg?e=9AI2fy

ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection – Basic Reference Model -- Part 2: Security Architecture”, 1989.

ISO/IEC 27000

Recomendaciones mínimas para política de respaldo de información - https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/publicaciones/respaldo-informacion