DESARROLLO DE UN PLAN DIRECTOR DE SEGURIDAD DE INFORMACIÓN PARA LA EMPRESA “AGUAS DE MANTA”.

PRESENTACIÓN DE LOS RESULTADOS DEL ANÁLISIS DE RIESGO Y LOS PROYECTOS.

Nombre Estudiante: Italo Hernández Valencia

Área: Sistemas de Gestión de la Seguridad de la Información.

Universitat Oberta de Catalunya

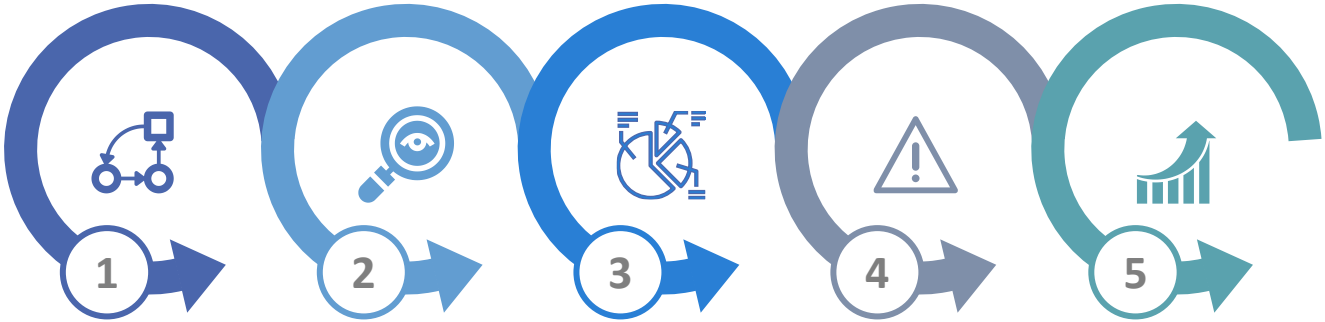
Metodología análisis de riesgos.

La metodología elegida para el despliegue de este Plan Director es **MAGERIT versión 3.0**

MAGERIT v3.0 es que expone sus resultados de manera cuantitativa, en porcentajes de riesgos y valores económicos, lo que convierte su producto final en un insumo fácil de consumir para los tomadores de decisiones.

Análisis de Riesgos.

Magerit V3.0



1. Inventario de Activos.

Se identificaron 48 activos de 6 distintas clases.

2. Análisis de amenazas.

Realizado mediante calificación por porcentajes y nivel de ocurrencia.

3. Cálculo de Impacto Potencial.

Valor del Activo multiplicado por porcentaje de impacto.

4. Cálculo del Riesgo

Basado en la frecuencia que pueda tener la ocurrencia de las amenazas.

5. Resultados

Riesgo potencial evaluado. Definición de umbral de riesgo aceptable.

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

1. Inventario y valoración de Activos.

Realizado con base en la cuantificación del valor de cada activo con escala de valoración económica , y su incidencia según los criterios de Confidencialidad , Integridad y Disponibilidad, puntuando del 1 al 10.

CLASE	ACTIVO	VALOR	C	I	D
Hardware	AACC de precisión.	Alto	4	8	10
	Cableado estructurado.	Alto	8	8	8
	CCTV (video vigilancia).	Medio	8	8	8
	Biométricos.	Muy bajo	8	6	8
	Dispositivos telefónicos.	Bajo	6	6	8
	Equipos de red.	Alto	10	10	8
	Estaciones de trabajo.	Alto	6	6	6
	Firewalls.	Alto	10	8	10
	Impresoras.	Bajo	4	2	4
	Routers.	Alto	6	6	10
	Servidor de archivos.	Alto	8	6	8
	Servidor e-mail.	Alto	8	6	8
	Servidor de telefonía IP.	Medio	2	8	10
	Servidor GIS	Medio	8	6	8
	Servidores de SCADA.	Alto	10	8	10
	Serv. virtualización.	Alto	10	8	10
	UPS	Medio	4	8	10

CLASE	ACTIVO	VALOR	C	I	D
Software	Antivirus.	Alto	8	8	8
	Aplicaciones internas.	Alto	8	8	10
	Herramientas de desarrollo	Bajo	8	10	4
	Programas utilitarios.	Medio	2	2	2
	Sistemas operativos.	Bajo	4	4	6
	Software e-mail	Alto	10	6	8
	Software de virtualizacion.	Medio	6	8	10
	Software SCADA.	Alto	6	8	10
Personal	Alta Gerencia .	Alto	2	8	8
	Guardianía.	Bajo	2	8	10
	Desarrolladores	Alto	10	8	8
	Personal externo.	Medio	2	8	6
	Personal operativo.	Alto	2	2	2
	Personal tecnológico.	Alto	10	8	8
	Personal administrativo.	Alto	10	8	8

CLASE	ACTIVO	VALOR	C	I	D
Instalaciones	Centros de Datos.	Muy alto	2	8	10
	Sala de Control Scada.	Alto	2	8	10
	Instalaciones	Muy alto	2	8	10
	Laboratorios	Alto	2	6	6
	Plantas de bombeo	Alto	2	8	6
Servicios	Correo electrónico.	Alto	8	6	8
	Infraestructura cloud.	Muy alto	10	6	10
	Portales tecnólogicos	Medio	10	6	10
	Sitio Web institucional.	Medio	8	6	8
	Switch transaccionales.	Alto	10	10	10
Datos	Datos de clientes (abonados).	Muy alto	8	10	10
	Datos de gestión interna.	Alto	6	8	10
	Datos financieros - contables.	Muy alto	8	10	10
	Información de usuarios	Bajo	2	2	2
	Registros de actividad	Medio	8	8	10

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

2. Análisis de Amenazas.

Construcción de una tabla granular de amenazas para la evaluación de cada uno de los activos identificados.

Esta calificación se establece bajo un criterio que mide su porcentaje de afectación y su nivel de ocurrencia.

Como ejemplo en esta presentación se expone una evaluación de las amenazas de un activo por cada clase.

HARDWARE				
[HW] - ACC DE PRECISIÓN.	**FA**	**35%**	**50%**	**100%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.3] Contaminación mecánica	FMB			100%
[I.4] Contaminación electromagnética	FMB			100%
[I.5] Avería de origen físico o lógico	FB			100%
[I.6] Corte del suministro eléctrico	FM			100%
[I.7] Condiciones inadecuadas de temperatura o humedad	FB			100%
[E.2] Errores del administrador	FMB	10%	50%	100%
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	FB			100%
[E.24] Caída del sistema por agotamiento de recurso	FB			100%
[E.25] Pérdida de equipos	FMB			100%
[A.6] Abuso de privilegios de acceso	FMB	25%	50%	100%
[A.7] Uso no previsto	FMB	25%	50%	100%
[A.11] Acceso no autorizado	FMB	25%	50%	
[A.23] Manipulación de los equipos	FMB	25%		100%
[A.24] Denegación de servicio	FMB			100%
[A.25] Robo	FMB	100%		100%
[A.26] Ataque destructivo	FMB			100%

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

2. Análisis de Amenazas.

SOFTWARE				
[SW] - ANTIVIRUS	**FA**	**85%**	**100%**	**100%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[i.5] Avería de origen físico o lógico	FM			100%
[E.1] Errores de los usuarios	FA	25%	100%	100%
[E.2] Errores del administrador	FM	25%	100%	100%
[E.8] Difusión de SW dañino	FMA	100%	100%	100%
[E.9] Errores de [re]-encaminamiento	FB	50%		
[E.10] Errores de secuencia	FMB		100%	
[E.15] Alteración accidental de la información	FB		100%	
[E.18] Destrucción de la información	FB			100%
[E.19] Fugas de información	FA	100%		
[E.20] Vulnerabilidades de los programas (SW)	FB	100%	100%	100%
[E.21] Errores de mantenimiento (SW)	FB		100%	100%
[A.5]Suplantación de la identidad del usuario	FB	100%	100%	
[A.6]Abuso de privilegios de acceso	FA	100%	100%	100%
[A.7]Uso no previsto	FA	100%	100%	100%
[A.8]Difusión de software dañino	FMB	100%	100%	100%
[A.9] [Re-]encaminamiento de mensajes	FMB			100%
[A.10]Alteración de secuencia	FMB		100%	
[A.11]Acceso no autorizado	FB	100%	100%	
[A.15]Modificación deliberada de la información	FM		100%	
[A.18]Destrucción de información	FMB			100%
[A.19]Divulgación de información	FB	100%		
[A.22]Manipulación de programas	FB	100%	100%	100%

PERSONAL.				
[P] - ALTA GERENCIA	**FM**	**60%**	**50%**	**55%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[E.19] Fugas de información	FA	80%		
[E.28] Indisponibilidad del personal	FA			50%
[A.28] Indisponibilidad del personal	FM			50%
[A.29] Extorsión	FM	50%	50%	50%
[A.30] Ingeniería social(picaresca)	FM	50%	50%	70%

INFRAESTRUCTURA				
[L] - CENTRO DE DATOS	**FM**	**60%**	**55%**	**100%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[N.1] Fuego	FMB			100%
[N.2] Daños por agua	FMB			100%
[N.*] Desastres naturales	FMB			100%
[I.1] Fuego	FMB			100%
[I.2] Daños por agua	FMB			100%
[I.*] Desastres industriales	FMB			100%
[I.11] electromagnéticas.	FMB	80%		
[E.15] Alteración de la información	FB		100%	
[E.18] Destrucción de información	FMB			100%
[E.19] Fugas de información	FB	80%		
[A.7] Uso no previsto	FB	50%	50%	100%
[A.11] Acceso no autorizado	FMB	50%	20%	
[A.15] Modificación información	FMB		50%	
[A.18] Destrucción de información	FMB			100%
[A.19] Divulgación de información.	FMB	50%		
[A.26] Ataque destructivo	FMB			100%
[A.27] Ocupación enemiga	FMB	50%		100%

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

2. Análisis de Amenazas.

SERVICIOS				
[S] - CORREO ELECTRÓNICO.	**FA**	**70%**	**70%**	**90%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[E.1] Errores de los usuarios	FMA	100%	100%	100%
[E.2] Errores del administrador	FB	100%	100%	100%
[E.9] Errores de [re]-encaminamiento	FB	50%		
[E.10] Errores de secuencia	FMB		50%	
[E.15] Alteración información	FB		50%	
[E.18] Destrucción de la información	FB			100%
[E.19] Fugas de información	FB			50%
[E.24] Caída del sistema por recursos	FB			100%
[A.5] Suplantación del usuario	FA	100%	100%	100%
[A.6] Abuso de privilegios de acceso	FMB	100%	60%	100%
[A.7] Uso no previsto	FB	50%	60%	50%
[A.9] [Re-]encaminamiento de mensajes	FMB	50%		
[A.10] Alteración de secuencia	FMB		50%	
[A.11] Acceso no autorizado	FM	30%	50%	
[A.13] Repudio	FB		100%	
[A.15] Modificación de la información	FB		50%	
[A.18] Destrucción de información	FB			100%
[A.19] Divulgación de información	FB	50%		
[A.24] Denegación de servicio	FMB			100%

DATOS				
[D] - DATOS DE CLIENTES (FACTURACIÓN)	**FB**	**70%**	**60%**	**100%**
LISTA DE AMENAZAS	**FREC**	**C**	**I**	**D**
[E.1] Errores de los usuarios	FM	100%	50%	100%
[E.2] Errores del administrador	FMB	100%	50%	100%
[E.15] Alteración accidental de la información	FM		50%	
[E.18] Destrucción de información	FB			100%
[E.19] Fugas de información	FMB	50%		
[A.5] Suplantación de la identidad del usuario	FMB	50%	100%	100%
[A.6] Abuso de privilegios de acceso	FM	50%	50%	100%
[A.11] Acceso no autorizado	FM	60%	60%	
[A.14] Interceptación de información (escucha)	FMB	50%		
[A.15] Modificación deliberada de la información	FB		60%	
[A.18] Destrucción de información	FMB			100%
[A.19] Divulgación de información	FA	100%		

3. Cálculo de Impacto Potencial.

Determinado por el daño causado sobre el activo por la materialización de la amenaza.

Este cálculo sirve como guía al momento de priorizar los proyectos a establecer el plan de acción a ejecutar.

Impacto = Valor del activo * Porcentaje de impacto.

CLASE	ACTIVO	CRITICIDAD			%IMPACTO			IMPACTO POTENCIAL		
		C	I	D	C	I	D	C	I	D
HARDWARE	AACC de precisión.	4	8	10	35%	50%	100%	1,4	4,0	10,0
	Cableado estructurado.	8	8	8	55%	50%	100%	4,4	4,0	8,0
	CCTV (video vigilancia).	8	8	8	35%	30%	100%	2,8	2,4	8,0
	Biométricos. (Acceso y Asistencia)	8	6	8	45%	35%	100%	3,6	2,1	8,0
	Dispositivos telefónicos.	6	6	8	50%	40%	100%	3,0	2,4	8,0
	Equipos de red.	10	10	8	50%	35%	100%	5,0	3,5	8,0
	Estaciones de trabajo.	6	6	6	50%	50%	100%	3,0	3,0	6,0
	Firewalls.	10	8	10	50%	25%	100%	5,0	2,0	10,0
	Impresoras.	4	2	4	50%	50%	100%	2,0	1,0	4,0
	Routers.	6	6	10	55%	25%	100%	3,3	1,5	10,0
	Servidor de archivos. (NAS)	8	6	8	100%	80%	100%	8,0	4,8	8,0
	Servidor de correo electrónico.	8	6	8	95%	80%	100%	7,6	4,8	8,0
	Servidor de telefonía IP.	2	8	10	90%	80%	100%	1,8	6,4	10,0
	Servidor Georeferenciación. (GIS)	8	6	8	90%	80%	100%	7,2	4,8	8,0
	Servidores de autómatas (SCADA).	10	8	10	90%	80%	100%	9,0	6,4	10,0
	Servidores de virtualización.	10	8	10	90%	80%	100%	9,0	6,4	10,0
	UPS	4	8	10	90%	80%	100%	3,6	6,4	10,0

CLASE	ACTIVO	CRITICIDAD			%IMPACTO			IMPACTO POTENCIAL		
		C	I	D	C	I	D	C	I	D
SOFTWARE	Antivirus.	2	8	8	85%	100%	100%	1,7	8,0	8,0
	Aplicaciones internas.	2	8	10	90%	100%	100%	1,8	8,0	10,0
	Herramientas de desarrollo .	10	8	8	90%	100%	100%	9,0	8,0	8,0
	Programas utilitarios.	2	8	6	90%	90%	100%	1,8	7,2	6,0
	Sistemas operativos.	2	2	2	90%	90%	100%	1,8	1,8	2,0
	Software de Correo electrónico.	10	8	8	85%	100%	100%	8,5	8,0	8,0
	Software de virtualizacion.	10	8	8	85%	100%	100%	8,5	8,0	8,0
	Software SCADA.	6	8	10	85%	100%	100%	5,1	8,0	10,0
PERSONAL	Alta Gerencia (Toma de decisiones).	2	8	8	60%	50%	55%	1,2	4,0	4,4
	Control de Accesos. (Guardianía)	2	8	10	50%	30%	30%	1,0	2,4	3,0
	Desarrolladores de software.	10	8	8	100%	50%	75%	10,0	4,0	6,0
	Personal externo. (proveedores, contratistas).	2	8	6	50%	30%	30%	1,0	2,4	1,8
	Personal operativo (personal obrero/limpieza).	2	2	2	50%	30%	30%	1,0	0,6	0,6
	Personal técnologico (infraestructura - soporte).	10	8	8	100%	50%	75%	10,0	4,0	6,0
	Usuarios finales. (personal administrativo).	10	8	8	50%	30%	30%	5,0	2,4	2,4
INSTALACIÓN	Centros de Datos.	2	8	10	60%	55%	100%	1,2	4,4	10,0
	Centro de Monitoreo (Sala de Control Scada).	2	8	10	60%	55%	100%	1,2	4,4	10,0
	Instalaciones estructurales. (Edificio, estaciones).	2	8	10	60%	55%	100%	1,2	4,4	10,0
	Laboratorios de Agua Potable.	2	6	6	60%	55%	100%	1,2	3,3	6,0
	Plantas de bombeo y tratamiento.	2	8	6	60%	55%	100%	1,2	4,4	6,0

3. Cálculo de Impacto Potencial.

Impacto = Valor del activo * Porcentaje de impacto.

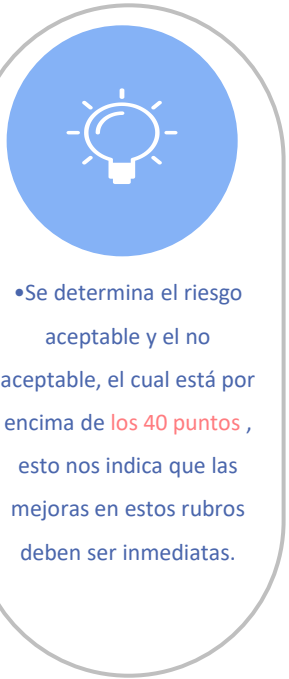
CLASE	ACTIVO	CRITICIDAD			%IMPACTO			IMPACTO POTENCIAL		
		C	I	D	C	I	D	C	I	D
SERVICIOS	Correo electrónico.	8	6	8	70%	70%	90%	5,6	4,2	7,2
	Infraestructura cloud.	10	6	10	40%	45%	45%	4,0	2,7	4,5
	Portales tecnólogicos publicados.	10	6	10	40%	45%	45%	4,0	2,7	4,5
	Sitio Web institucional.	8	6	8	40%	45%	45%	3,2	2,7	3,6
	Switch transaccionales.	10	10	10	40%	45%	45%	4,0	4,5	4,5
DATOS.	Datos de clientes (abonados).	8	10	10	70%	60%	100%	5,6	6,0	10,0
	Datos de gestión interna.	6	8	10	70%	60%	100%	4,2	4,8	10,0
	Datos financieros - contables.	8	10	10	70%	60%	100%	5,6	6,0	10,0
	Información de usuarios (personal).	2	2	2	20%	10%	15%	0,4	0,2	0,3
	Registros de actividad (logs).	8	8	10	70%	60%	100%	5,6	4,8	10,0

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

4. Cálculo del Riesgo Potencial.

Posterior a calcular el impacto potencial ahora contamos con un insumo necesario para poder calcular el riesgo potencial basado en la frecuencia que pueda tener la ocurrencia de las amenazas proyectadas y su valor numérico.

Riesgo = Frecuencia x Impacto.



•Se determina el riesgo aceptable y el no aceptable, el cual está por encima de los 40 puntos , esto nos indica que las mejoras en estos rubros deben ser inmediatas.

CLASE	ACTIVO	FREC.		IMPACTO POTENCIAL			RIESGO POTENCIAL		
		FREC	VAL	C	I	D	C	I	D
HARDWARE	AACC de precisión.	FA	10	1,4	4,0	10,0	14,00	40,00	100
	Cableado estructurado.	FMB	0,01	4,4	4,0	8,0	0,04	0,04	0,08
	CCTV (video vigilancia).	FMB	0,01	2,8	2,4	8,0	0,03	0,02	0,08
	Dispositivos biométricos. (Acceso y Asistencia)	FM	1	3,6	2,1	8,0	3,60	2,10	8,00
	Dispositivos telefónicos.	FMB	0,01	3,0	2,4	8,0	0,03	0,02	0,08
	Equipos de red. (ACCES POINT, SWITCH)	FB	0,1	5,0	3,5	8,0	0,50	0,35	0,80
	Estaciones de trabajo.	FM	1	3,0	3,0	6,0	3,00	3,00	6,00
	Firewalls.	FM	1	5,0	2,0	10,0	5,00	2,00	10,00
	Impresoras.	FMB	1	2,0	1,0	4,0	2,00	1,00	4,00
	Routers.	FB	0,1	3,3	1,5	10,0	0,33	0,15	1,00
	Servidor de archivos. (NAS)	FA	10	8,0	4,8	8,0	80,00	48,00	80,00
	Servidor de correo electrónico.	FA	10	7,6	4,8	8,0	76,00	48,00	80,00
	Servidor de telefonía IP.	FMB	1	1,8	6,4	10,0	1,80	6,40	10,00
	Servidor Georeferenciación. (GIS)	FB	0,1	7,2	4,8	8,0	0,72	0,48	0,80
	Servidores de autómatas (SCADA).	FB	0,1	9,0	6,4	10,0	0,90	0,64	1,00
	Servidores de virtualización.	FB	0,1	9,0	6,4	10,0	0,90	0,64	1,00
	UPS	FA	10	3,6	6,4	10,0	36,00	64,00	100

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

4. Cálculo del Riesgo Potencial.

CLASE	ACTIVO	FREC.		IMPACTO POTENCIAL			RIESGO POTENCIAL		
		FRE	VAL	C	I	D	C	I	D
SOFTWARE.	Antivirus.	FA	10	1,7	8,0	8,0	16,92	80,00	80,00
	Aplicaciones internas.	FA	10	1,8	8,0	10,0	18,08	80,00	100
	Herramientas de desarrollo .	FA	10	9,0	8,0	8,0	90,38	80,00	80,00
	Programas utilitarios.	FA	10	1,8	7,2	6,0	18,08	72,27	60,00
	Sistemas operativos.	FM	1	1,8	1,8	2,0	1,81	1,81	2,00
	Software de Correo electrónico.	FM	1	8,5	8,0	8,0	8,46	8,00	8,00
	Software de virtualizacion.	FM	1	8,5	8,0	8,0	8,46	8,00	8,00
	Software SCADA.	FB	0,1	5,1	8,0	10,0	0,51	0,80	1,00
PERSONAL.	Alta Gerencia	FM	1	1,2	4,0	4,4	1,20	4,00	4,40
	(Guardianía)	FM	1	1,0	2,4	3,0	1,00	2,40	3,00
	Desarrolladores de software.	FA	10	10,0	4,0	6,0	100	40,00	60,00
	Personal externo	FM	1	1,0	2,4	1,8	1,00	2,40	1,80
	Personal operativo	FM	1	1,0	0,6	0,6	1,00	0,60	0,60
	Personal técnologico	FA	10	10,0	4,0	6,0	100	40,00	60,00
	Usuarios finales. (personal administrativo).	FA	10	5,0	2,4	2,4	50,00	24,00	24,00

Riesgo = Frecuencia x Impacto.

CLASE	ACTIVO	FREC.		IMPACTO POTENCIAL			RIESGO POTENCIAL		
		FRE	VAL	C	I	D	C	I	D
INSTALACIONES	Centros de Datos.	FM	1	1,2	4,4	10,0	1,20	4,40	10,00
	Centro de Monitoreo	FM	1	1,2	4,4	10,0	1,20	4,40	10,00
	Instalaciones	FB	0,1	1,2	4,4	10,0	0,12	0,44	1,00
	Laboratorios de Agua Potable.	FB	0,1	1,2	3,3	6,0	0,12	0,33	0,60
	Plantas de bombeo y tratamiento.	FB	0,1	1,2	4,4	6,0	0,12	0,44	0,60
SERVICIOS	Correo electrónico.	FA	10	5,6	4,2	7,2	56,00	42,00	72,00
	Infraestructura cloud.	FA	10	4,0	2,7	4,5	40,00	26,73	45,00
	Portales tecnólogicos	FA	10	4,0	2,7	4,5	40,00	26,73	45,00
	Sitio Web institucional.	FA	10	3,2	2,7	3,6	32,00	26,73	36,00
	Switch transaccionales.	FA	10	4,0	4,5	4,5	40,00	44,55	45,00
DATOS	Datos de clientes (abonados).	FB	0,1	5,6	6,0	10,0	0,56	0,60	1,00
	Datos de gestión interna.	FB	0,1	4,2	4,8	10,0	0,42	0,48	1,00
	Datos financieros - contables.	FB	0,1	5,6	6,0	10,0	0,56	0,60	1,00
	Información de usuarios (personal).	FB	0,1	0,4	0,2	0,3	0,04	0,02	0,03
	Registros de actividad (logs).	FB	0,1	5,6	4,8	10,0	0,56	0,48	1,00

RIESGO NO ACEPTABLE

RIESGO ACEPTABLE

5. Propuestas de Proyectos.

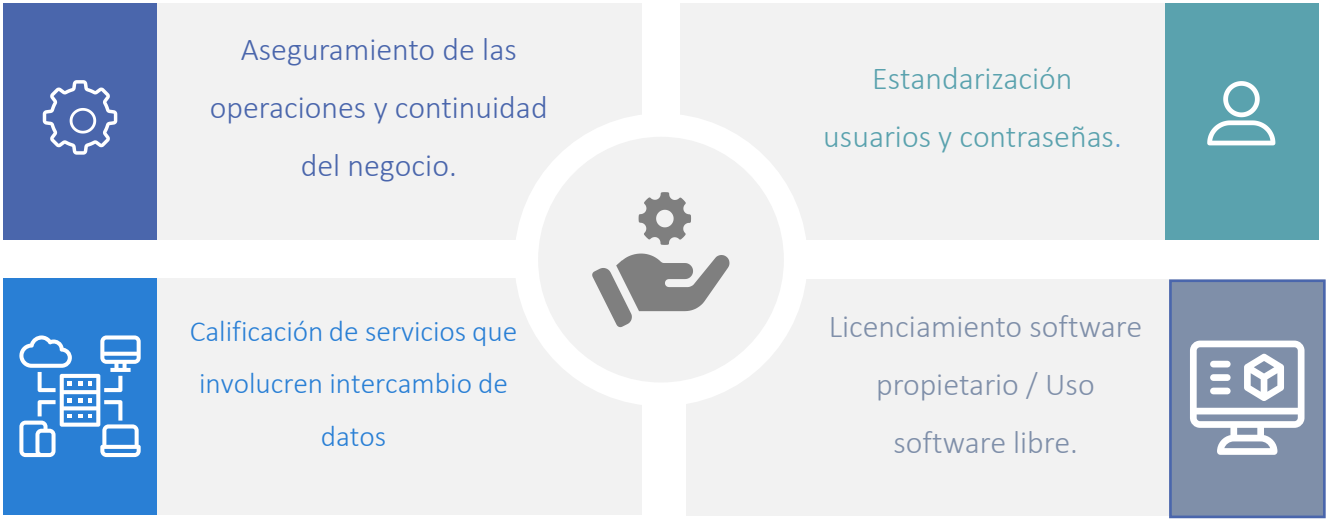
El análisis de riesgos realizado en la sección anterior es el disparador y punto de origen para el despliegue nuestros proyectos que forman parte de la propuesta

El riesgo potencial asociado a cada activo nos provee un panorama más claro acerca de los puntos débiles de la organización en temas de seguridad de la información.

Estos proyectos buscan: controlar el riesgo, que sus índices se reduzcan considerablemente y que mantengan los activos en un nivel por debajo del riesgo aceptable.

Propuestas de Proyectos.

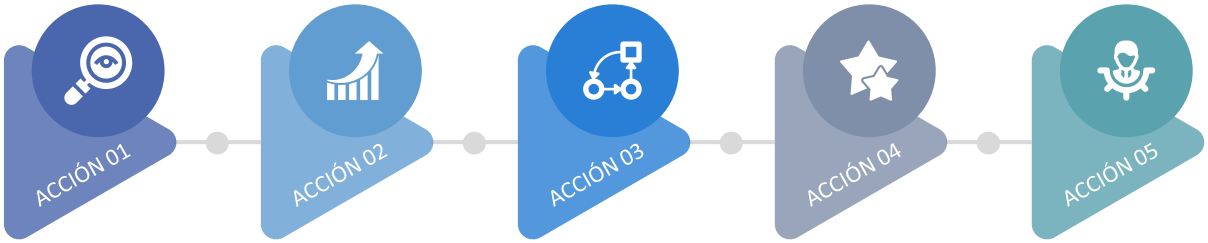
Los proyectos propuestos son cuatro:



Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

PR1: ASEGURAMIENTO DE LAS OPERACIONES Y CONTINUIDAD DEL NEGOCIO.

OBJETIVO: Documentar procedimientos que soporten la implementación de controles que respalden la política de seguridad .
BENEFICIOS: Aseguramiento y protección de datos de la organización - **horas de servicios tecnológicos ininterrumpidas.**
DURACIÓN: **6** Semanas.



STEP # 01
Definición de un Plan de respaldo de datos sensibles almacenados en infraestructura.

STEP # 02
Crear un esquema de continuidad de negocio y recuperación ante desastres.

STEP # 03
Tomar acciones respecto al respaldo de suministro eléctrico.

STEP # 04
Definir planes de mantenimiento para climatización de centro de datos y cuartos de equipos.

STEP # 05
Definir políticas de accesos areas restringidas.

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

Universitat Oberta de Catalunya

PR2 : ESTANDARIZACIÓN DE USUARIOS Y CONTRASEÑAS.

OBJETIVO: Documentar procedimientos que soporten la implementación de controles que respalden la política de seguridad .

BENEFICIOS: Minimizar el riesgo del uso de usuarios genéricos , anónimos , privilegios inadecuados y accesos no autorizados a equipos y sistemas de información..

DURACIÓN: 8 Semanas.

ACCIÓN #1

Socializar política de usuarios y contraseñas..

ACCIÓN #3

Definición de umbrales y directivas de seguridad para autenticación de usuarios.

ACCIÓN #2

Expedición de acuerdo de confidencialidad y uso de medios electrónicos.

ACCIÓN #4

Definición de un plan de inducción/capacitación para usuarios finales y personal de nuevo ingreso, concerniente a responsabilidad y buen uso de usuarios y contraseñas.

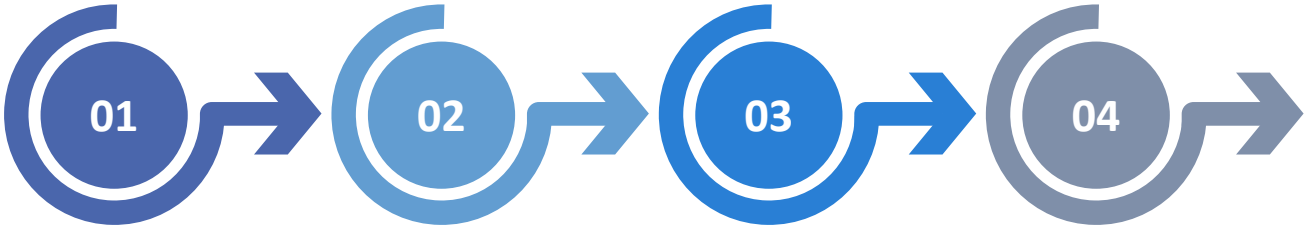
Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

PR3: REVISIÓN Y CALIFICACIÓN DE SERVICIOS QUE INVOLUCREN INTERCAMBIO DE DATOS.

OBJETIVO: Establecer un esquema para calificación de requisitos de seguridad de información para servicios internos o externos que involucren intercambio de datos..

BENEFICIOS: Proteger la infraestructura tecnológica de la organización frente a ataques o acciones fraudalentas - Aseguramiento y protección de los datos de la organización.

DURACIÓN: 6 Semanas.



#1

Definición de requisitos mínimos de seguridad para servicios tecnológicos antes de su adquisición.

#2

Realizar inventario de puertos necesarios que utilicen los servicios..

#3

Definir privilegios mínimos durante las etapas de testeo de los servicios.

#4

Documentar plan de reverso (roll-back) por cada nueva implementación, antes de la etapa de producción o publicación.

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

Universitat Oberta de Catalunya

PR4: LICENCIAMIENTO DE SOFTWARE PROPIETARIOS / USO DE SOFTWARE LIBRE.

OBJETIVO: Contar con software utilitario licenciado.

BENEFICIOS: Minimizar el riesgo de malware, virus y código malicioso que pongan en riesgo la infraestructura tecnológica de la organización. - Contar con software legalmente reconocido y funcional.

DURACIÓN: 8 Semanas.

ACCIÓN # 01

Inventario de software necesario para las actividades de la organización.

ACCIÓN # 02

Análisis de alternativas para solventar las necesidades mediante software libre.

ACCIÓN # 03

Definir un procedimiento de revisión de equipos ajenos a la organización antes de concederles acceso a la red de datos institucional.

ACCIÓN # 04

Eliminar de las estaciones de trabajo cracks y parches con código malicioso que simulen licenciamiento.

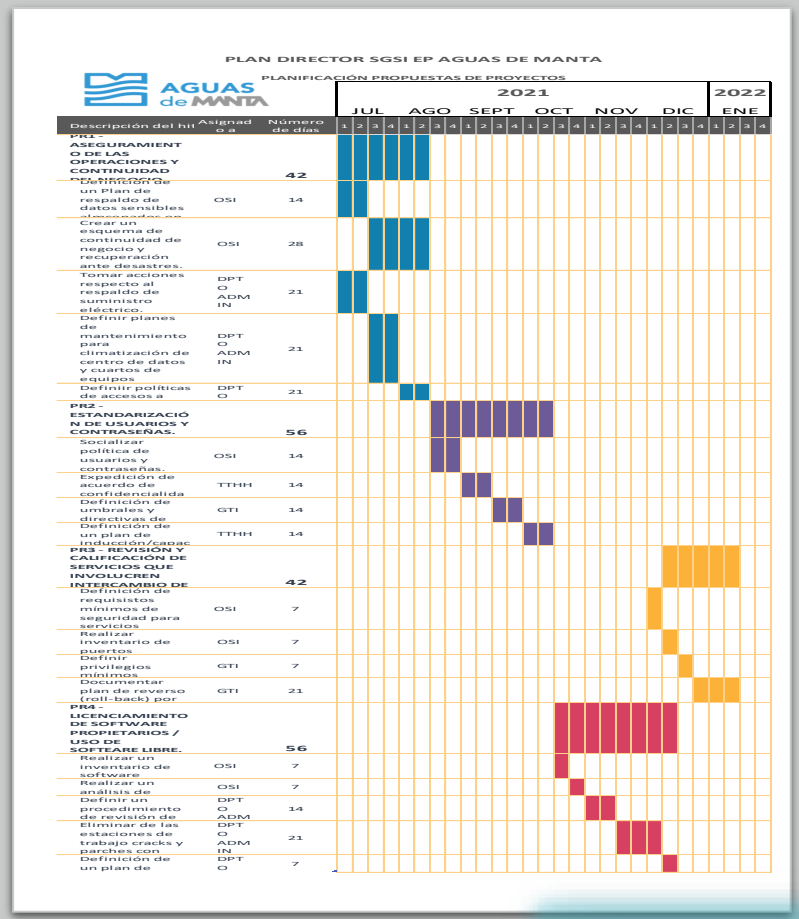
ACCIÓN # 05

Capacitación para usuarios finales.

Planificación.

- Para la comprensión de el despliegue de los proyectos establecemos el siguiente diagrama de Gantt con la intención de resumir el desarrollo programado de los proyectos en el lapso de meses desde Julio 2021 a Enero 2022.

- La siguiente tabla detalla actividades a realizar , los responsables de las mismas y el número de días contemplados para el desarrollo de estas.



Descripción del hit	Asignado a	Número de días
PR1 - ASEGURAMIENTO DE LAS OPERACIONES Y CONTINUIDAD		**42**
Definición de un Plan de respaldo de datos sensibles	OSI	14
Crear un esquema de continuidad de negocio y recuperación ante desastres.	OSI	28
Tomar acciones respecto al respaldo de suministro eléctrico.	DPTO ADMIN	21
Definir planes de mantenimiento para climatización de centro de datos y cuartos de equipos	DPTO ADMIN	21
Definiir políticas de accesos a	DPTO	21
PR2 - ESTANDARIZACIÓN DE USUARIOS Y CONTRASEÑAS.		**56**
Socializar política de usuarios y contraseñas.	OSI	14
Expedición de acuerdo de confidencialida	TTHH	14
Definición de umbrales y directivas de	GTI	14
Definición de un plan de inducción/capac	TTHH	14
PR3 - REVISIÓN Y CALIFICACIÓN DE SERVICIOS QUE INVOLUCREN INTERCAMBIO DE		**42**
Definición de requisistos mínimos de seguridad para servicios	OSI	7
Realizar inventario de puertos	OSI	7
Definir privilegios mínimos	GTI	7
Documentar plan de reverso (roll-back) por	GTI	21
PR4 - LICENCIAMIENTO DE SOFTWARE PROPIETARIOS / USO DE SOFTEARE LIBRE.		**56**
Realizar un inventario de software	OSI	7
Realizar un análisis de	OSI	7
Definir un procedimiento de revisión de	DPTO ADMIN	14
Eliminar de las estaciones de trabajo cracks y parches con	DPTO ADMIN	21
Definición de un plan de	DPTO	7

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

6. Auditoría de cumplimiento.

No conformidades.

Como referencia para nuestro análisis de no conformidades establecemos los siguientes criterios previo al despliegue de la auditoría propiamente dicha.

TIPO	DESCRIPCIÓN
No conformidad mayor	Se incumple por completo un apartado del estándar
No conformidad menor	Se incumple un punto del estándar o se incumple un procedimiento propio de la organización.
Observación	No se incumple nada, pero si no se hace un tratamiento adecuado, en el futuro se puede convertir en no conformidad menor
Oportunidad de mejora	Es solo una recomendación, que nunca se convertirá ni en observación ni en no conformidad.

Establecemos las no conformidades encontradas antes de los puntos de mejora. Las No Conformidades detectadas en el transcurso de la auditoria.

6. Auditoría de cumplimiento.

No conformidades.

No. No Conformidad:	1
Área:	Seguridad ligada a RR.HH..
Tipo de No Conformidad:	MAYOR
Control incumplido:	A.7.2.2 Concienciación , educación y capacitación en SI
Descripción:	No se realiza el procedimiento de inducción ni capacitación para el personal en temas de seguridad de la información. El manejo de responsabilidades en cuanto a los roles del personal no es perceptible.
Acción Correctiva:	Realizar seguimiento acerca de los planes de capacitación y procedimientos establecidos en cuanto a roles y responsabilidades.
Fecha de Revisión:	20-abr-21

No. No Conformidad:	2
Área:	Seguridad ligada a RR.HH..
Tipo de No Conformidad:	MAYOR
Control incumplido:	A.7.2.3 Proceso disciplinario.
Descripción:	No existe procedimiento disciplinario para el desacato a las políticas de seguridad, ni para sancionar acciones que deriven en brechas de seguridad.
Acción Correctiva:	Realizar seguimiento acerca de los procedimientos establecidos en cuanto a sanciones administrativas.
Fecha de Revisión:	27-abr-21

No. No Conformidad:	3
Área:	Control de Acceso.
Tipo de No Conformidad:	MENOR
Control incumplido:	A 9.2.4 Gestión de la información secreta autenticación de usuario
Descripción:	Los sistemas de información y Las estaciones de trabajo cuentan con un sistema de autenticación pero las claves genéricas conocidas por el personal en su mayoría imposibilitan la confidencialidad de aquello.
Acción Correctiva:	Desplegar y hacer cumplir a cabalidad la política de seguridad de información, apartado usuarios y contraseñas, fijar obligatoriedad de cumplimiento al personal.
Fecha de Revisión:	04-may-21

No. No Conformidad:	4
Área:	Control de Acceso.
Tipo de No Conformidad:	MENOR
Control incumplido:	A 9.4.1 Restricción de acceso a información.
Descripción:	Los accesos a información sensible no se encuentran correctamente mapeados, y los privilegios de acceso a aplicaciones son muy generales.
Acción Correctiva:	Establecer perfiles de acceso y privilegios según las atribuciones y necesidades de usuarios.
Fecha de Revisión:	04-may-21

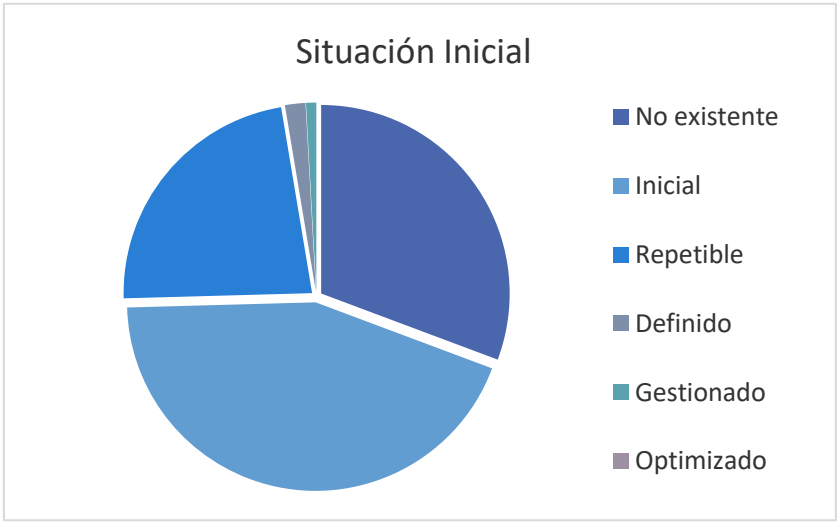
6. Auditoría de cumplimiento.

Resultados.

Las siguientes tablas e ilustraciones proveen una visión más comprensible del estado de los controles antes y después de la implementación del plan director.

ESTADO INICIAL DE LOS CONTROLES IS027001.

SITUACION INICIAL		
NIVEL (L)	CANT. COTROLES	%
No existente	35	30,70
Inicial	50	43,86
Repetible	26	22,81
Definido	2	1,75
Gestionado	1	0,88
Optimizado	0	0,00



6. Auditoría de cumplimiento.

Resultados.

ESTADO FINAL DE LOS CONTROLES IS027001.

SITUACION FINAL		
NIVEL (L)	CANT. COTROLES	%
No existente	0	0,00
Inicial	0	0,00
Repetible	26	22,81
Definido	65	57,02
Gestionado	21	18,42
Optimizado	2	1,75

Acerca de:

Autor: ITALO HERNÁNDEZ VALENCIA – MAYO 2021.

LINKEDin: italohernandez

Esta presentación es un extracto de los capítulos 3 y 4 del documento:

PLAN DIRECTOR DE SEGURIDAD PARA LA EP AGUAS DE MANTA :
https://drive.google.com/open?id=13p8y0ISs4EHuR_TfaYhuNSCTtGN6LjTS

UOC - MAYO 2021

Universitat Oberta de Catalunya