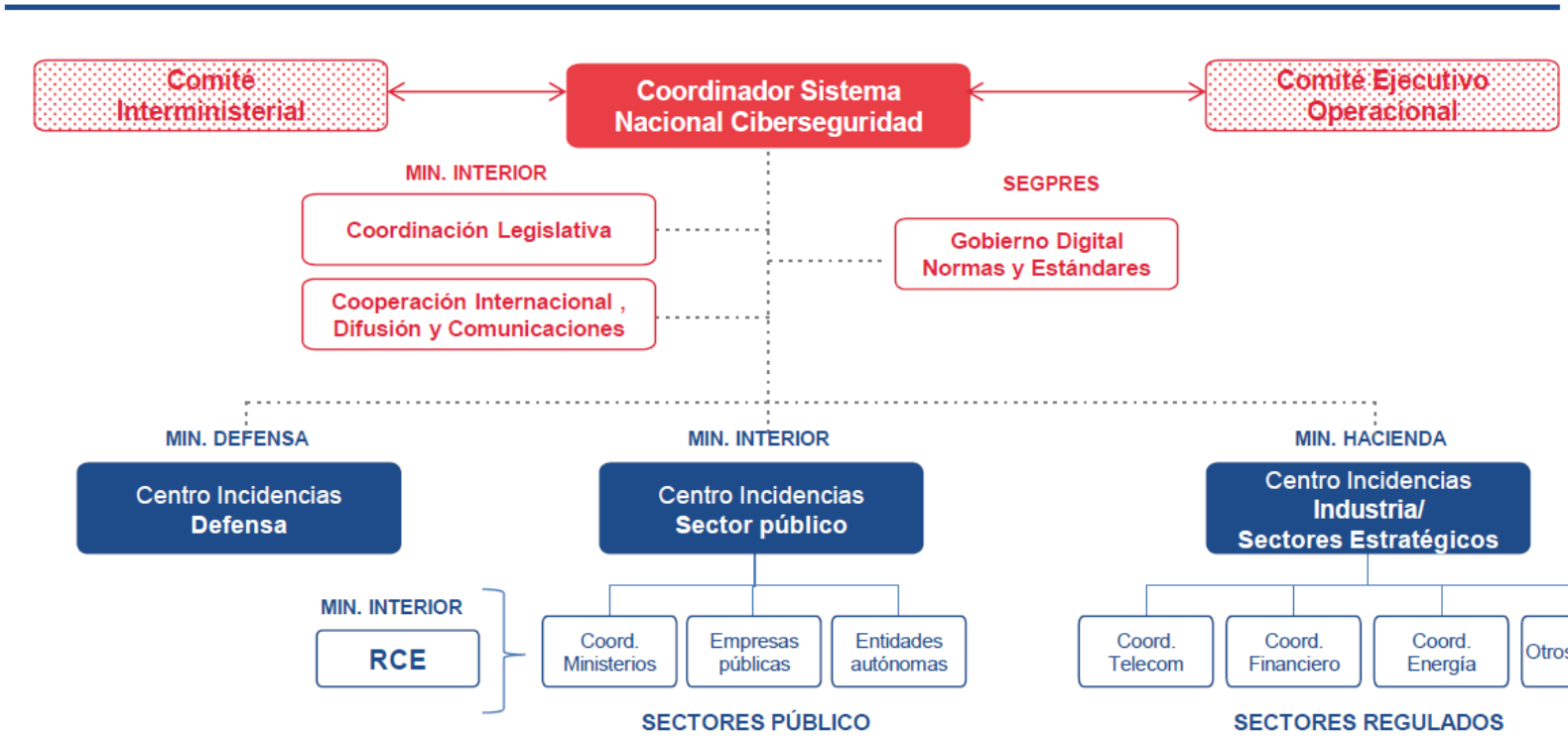
CIBERSEGURIDAD EL RETO DE LA IMPLEMENTACIÓN

Juan Carlos Gutiérrez R.
Encargado de la Oficina de Seguridad de la Información

Algo para partir….

1. 16 de los 19 anexos OACI, podrían contener incorporadas materias de ciberseguridad
2. Debemos dar un enfoque transversal
3. Se requiere contar con un marco de referencia que oriente a las organizaciones
4. Los riesgos de ciberseguridad ampliaron el campo de análisis, definiendo nuevos escenarios
5. Análisis de Riesgo orientado a activos
6. Trabajo en equipo
7. No identifiquemos un área especifica (se explica)

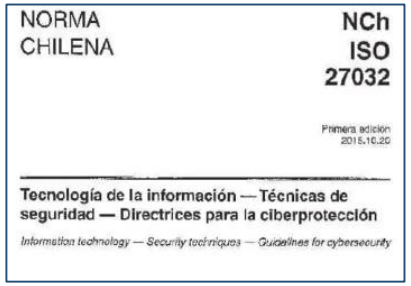
El estado de chile



DGAC
CHILE

- Lineamiento político del Estado de Chile en materia de Ciberseguridad
- Objetivo es tener un Ciberespacio libre, abierto, seguro y resiliente a través de acciones que permitan identificar y gestionar riesgos
- Establece 5 ejes estratégicos: Infraestructura, Legislación, Difusión, Colaboración Internacional y Desarrollo de Industria
- Establece proyectos de ley tales como: Nueva Ley de Delitos Informáticos; Ley Marco de Ciberseguridad; Ley de Infraestructura Crítica para Ciberseguridad; Protección de Datos Personales
- Lineamientos para definir un modelo de gobernanza que determine las relaciones interministeriales y el rol especifico de los organismos al implementar esas funciones.

DGAC
CHILE


NORMA CHILENA

NCh ISO 27032

Primera edición 2015.10.20

Tecnología de la información — Técnicas de seguridad — Directrices para la ciberprotección

Information technology — Security techniques — Guidelines for cybersecurity


NORMA CHILENA **NCh-ISO 27001**

Segunda edición 2013.10.25

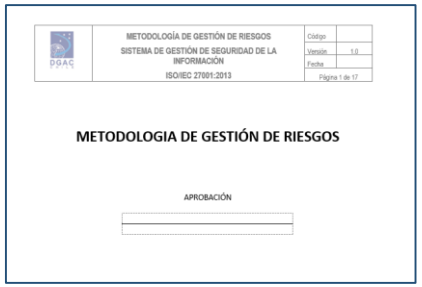
Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos

Information technology - Security techniques - Information security management systems - Requirements

POLÍTICA NACIONAL DE CIBERSEGURIDAD


Dirección General de Aeronáutica Civil
Norma Técnica de Ciberseguridad
Código: DGAC-001
Versión: 1.0
Página 1 de 11

NORMA TÉCNICA DE CIBERSEGURIDAD AERONÁUTICA


METODOLOGÍA DE GESTIÓN DE RIESGOS
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
ISO/IEC 27001:2013
Código
Versión 1.0
Fecha
Página 1 de 17

METODOLOGIA DE GESTIÓN DE RIESGOS

APROBACIÓN


Plan Director de Seguridad de la Información y Ciberseguridad
Dirección General de Aeronáutica Civil

DGAC
CHILE

PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

DIRECCIÓN GENERAL DE AERONÁUTICA CIVIL

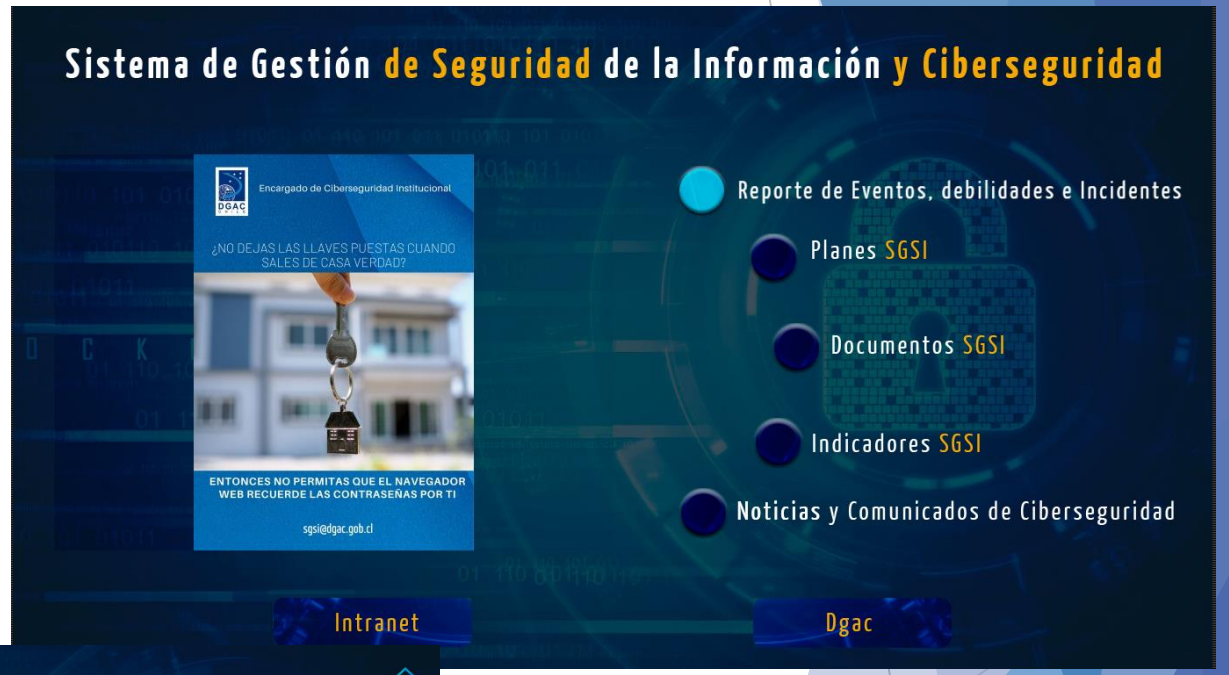
2022

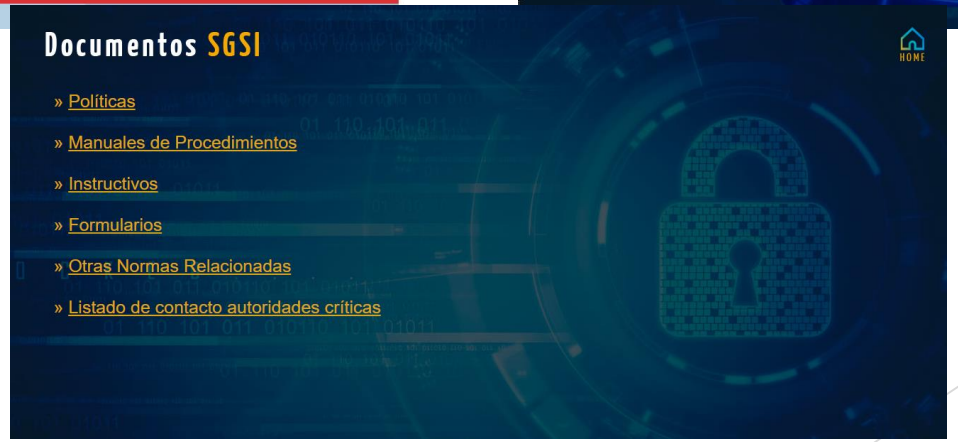
NORMAS ISO vigentes al 2018 en el Instituto Nacional de Normalización (INN), para Ciberseguridad

NCh-ISO27000:2014→Sistemas de gestión de seguridad de la información - Visión general y vocabulario.
NCh-ISO27001:2013→Sistemas de gestión de la seguridad de la información - Requisitos.
NCh-ISO27002:2013→Código de prácticas para los controles de seguridad de la información.
NCh-ISO27003:2014→Guía de implementación del sistema de gestión de seguridad de la información.
NCh-ISO27005:2014→Gestión del riesgo de seguridad de la información .
NCh-ISO27013:2013→Orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
NCh-ISO27014:2015→Gobernanza de seguridad de la información.
NCh-ISO27018:2015→Código de práctica para la protección de la información personal de identificación (PII) en nubes públicas que desempeñen el rol de procesadores de PII.
NCh-ISO27031:2015→Directrices para la preparación de las tecnologías de la informática y comunicaciones para la continuidad del negocio.
NCh-ISO27032:2015→Directrices para la ciberprotección.
NCh-ISO27036/1:2015→Seguridad de la información en las relaciones con los proveedores - Parte 1: Visión general y conceptos
NCh-ISO27036/2:2015→Seguridad de la información para las relaciones con proveedores - Parte 2: Requisitos´.
NCh-ISO27036/3:2015→Seguridad de la información para las relaciones con proveedores - Parte 3: Directrices para la seguridad en la cadena de suministro de las tecnologías de la información y la comunicación.
NCh-ISO27040:2015→Seguridad de almacenamiento.
NCh-ISO27003:2014→Guía de implementación del sistema de gestión de seguridad de la información.
NCh-ISO27005:2014→Gestión del riesgo de seguridad de la información.
NCh-ISO27031:2015→Directrices para la preparación de las tecnologías de la informática y comunicaciones para la continuidad del negocio.
NCh-ISO27037:2015→Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.

DGAC CHILE


English
CSIRT
Quiénes somos
Acerca de Ciberseguridad
Preguntas Frecuentes
Decretos de Ciberseguridad
Eventos
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática
Contáctanos al 1510
REGISTRAR UN INCIDENTE
¿Cómo y cuándo reportar?
¿Qué es CSIRT?
VER VIDEO INSTITUCIONAL
Noticias
publicado el 29 de agosto de 2022
ALERTA DE SEGURIDAD CIBERNÉTICA: INCIDENTE EN SERVICIO PÚBLICO
El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, informa sobre un incidente en progreso que afecta a un servicio del gobierno, durante la jornada del jueves 25 de agosto, el cual ha interrumpido el funcionamiento de sus sistemas y servicios en línea.
VER MÁS
Alertas
publicado el 31 de agosto de 2022
2CMV22-00337-01 CSIRT alerta ante campaña de phishing con falso documento de pago
publicado el 31 de agosto de 2022
2CMV22-00336-01 CSIRT alerta ante campaña de phishing con falso documento de pago
VER MÁS


Sistema de Gestión de Seguridad de la Información y Ciberseguridad
Encargado de Ciberseguridad Institucional
¿NO DEJAS LAS LLAVES PUESTAS CUANDO SALES DE CASA VERDAD?
ENTONCES NO PERMITAS QUE EL NAVEGADOR WEB RECUERDE LAS CONTRASEÑAS POR TI
sgsi@dgac.gob.cl
Reporte de Eventos, debilidades e Incidentes
Planes SGSI
Documentos SGSI
Indicadores SGSI
Noticias y Comunicados de Ciberseguridad
Intranet
Dgac


Documentos SGSI
HOME
» Políticas
» Manuales de Procedimientos
» Instructivos
» Formularios
» Otras Normas Relacionadas
» Listado de contacto autoridades críticas

Cual es el error mas frecuente

Con frecuencia descuidamos lo que no vemos, no entendiendo que son muy importantes

DGAC CHILE

Puedo usar otros Marcos y guias de Referencia ?

COBIT 5

ISO 27001

NITS

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR	gestión del riesgo de seguridad cibernética.	**ID.GV-2:** Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4**-1 controles de todas las familias de control de seguridad
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Cláusula 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

Que es un sistema de gestión

"Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos, y procesos para lograr estos objetivos."

ISO 9.000

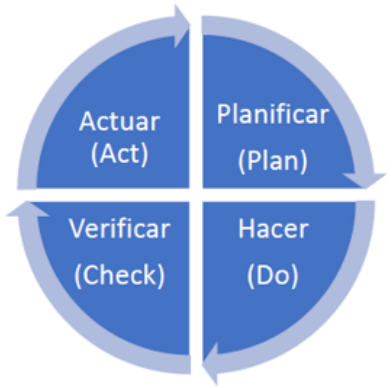
"Un SGSI (Sistema de Gestión de la Seguridad de la Información) consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización."

ISO 27.000

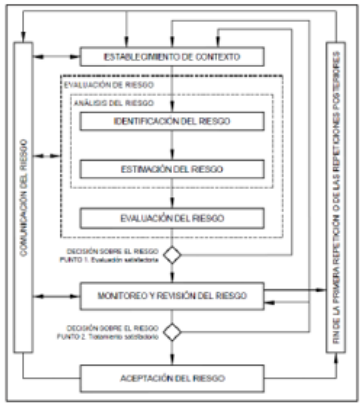
"Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio."

ISO 27.000

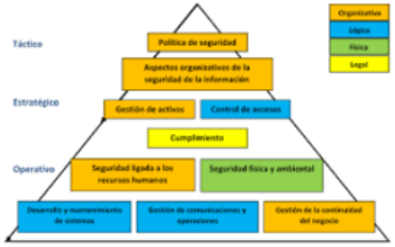
Que ofrece la ISO 27001



Visión de Procesos alineada al ciclo PDCA



Enfoque de Riesgos



Controles de Seguridad de la Información

Clausula 1:	Objeto y campo de aplicación
Clausula 2:	Referencias normativas
Clausula 3:	Términos y definiciones
Clausula 4:	Contexto de la organización
Clausula 5:	Liderazgo
Clausula 6:	Planificación
Clausula 7:	Soporte
Clausula 8:	Operación
Clausula 9:	Evaluación del desempeño
Clausula 10:	Mejora

Metodología Estandarizada

DGAC
CHILE

CALIDAD

Políticas Complementarias – A.5.1.1 ISO 27.002

ISO 27002:2013 DOMINIOS	
A5	Política de Seguridad de la Información
A6	Organización de la seguridad de la información
A7	Seguridad de los RRHH
A8	Gestión de activos
A9	Control de accesos
A10	Criptografía
A11	Seguridad física y ambiental
A12	Seguridad en las operaciones
A13	Seguridad en las comunicaciones
A14	Adquisición, desarrollo y mantenimiento de los sistemas
A15	Relaciones con proveedores
A16	Gestión de incidentes de seguridad de la información
A17	Aspectos de seguridad de la inf. en continuidad de negocio
A18	Cumplimiento

a) control de acceso (véase el capítulo 9);

b) clasificación de la información (y su manejo) (véase 8.2);

c) seguridad física y ambiental (véase el capítulo 11);

d) temas orientados al usuario final tales como:

   1) uso adecuado de activos (véase 8.1.3),
   2) puesto de trabajo despejado y pantalla limpia (véase 11.2.9),
   3) transferencia de información (véase 13.2.1),
   4) dispositivos móviles y teletrabajo (véase 6.2),
   5) restricciones de instalación y uso de software (véase 12.6.2);

e) copias de respaldo (véase 12.3);

f) transferencia de información (véase 13.2);

g) protección ante el software malicioso (*malware*) (véase 12.2);

h) gestión de vulnerabilidades técnicas (véase 12.6.1);

i) controles criptográficos (véase el capítulo 10);

j) seguridad de las comunicaciones (véase el capítulo 13);

k) privacidad y protección de la información identificativa de personas (véase 18.1.4);

l) relaciones con proveedores (véase el capítulo 15).

Controle de Seguridad de la Información

- Ofrece 114 controles de seguridad de la información.
- Se implementan en virtud de los riesgos del negocio
- Ofrecen una línea base de controles necesaria para cualquier organización

Ciclo PDCA

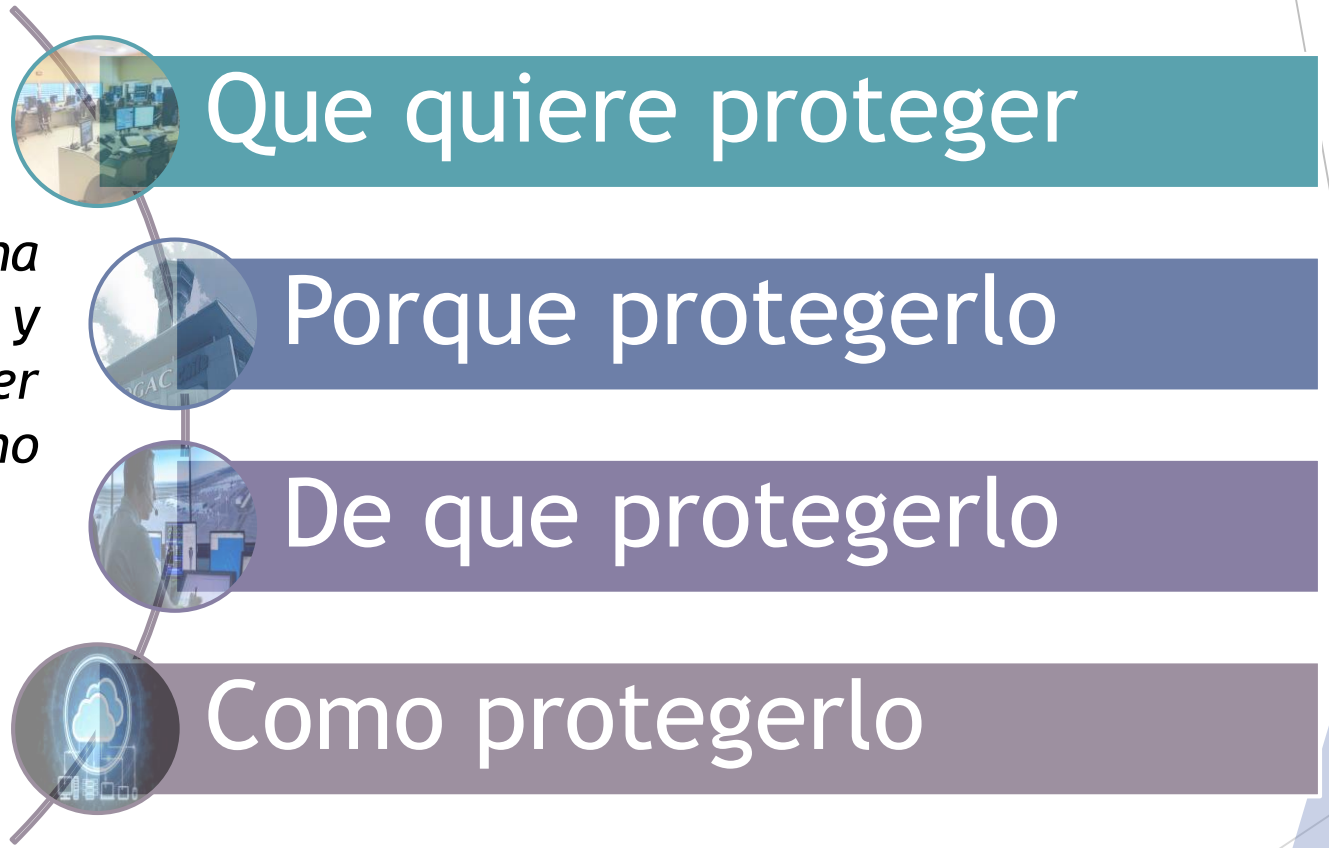
- ✓ Permite a una organización asegurarse de que sus procesos cuenten con recursos y se gestionen adecuadamente.

- ✓ Posibilita que las oportunidades de mejora se determinen y se actúe en consecuencia.

- ✓ La aplicación del enfoque a procesos en un sistema de gestión permite:
  - A. La comprensión en el cumplimiento de los requisitos.
  - B. La consideración de los procesos integrado.
  - C. El logro del desempeño eficaz del proceso.
  - D. La mejora de los procesos con base en la evaluación de los datos, la información y objetivos.

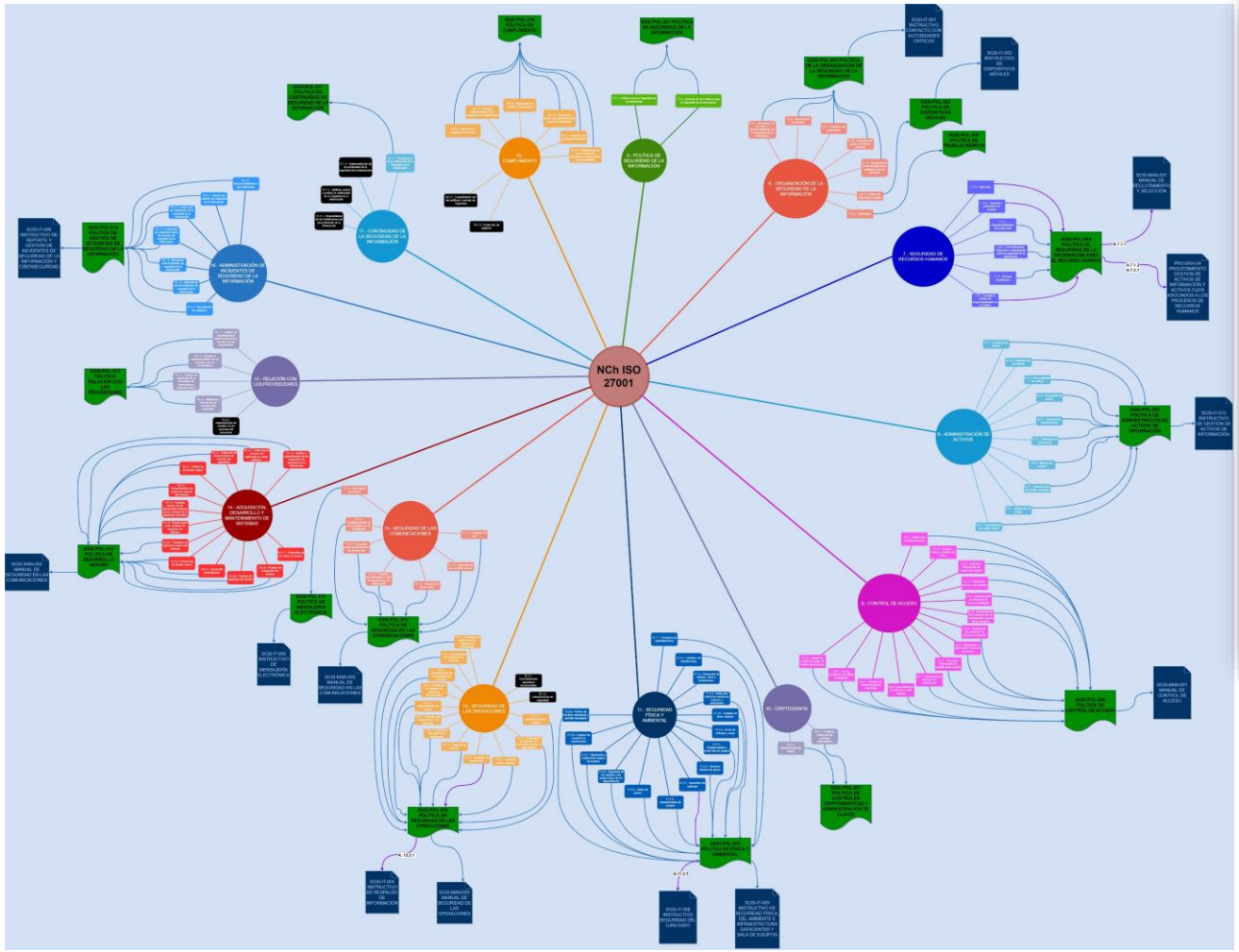
https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html

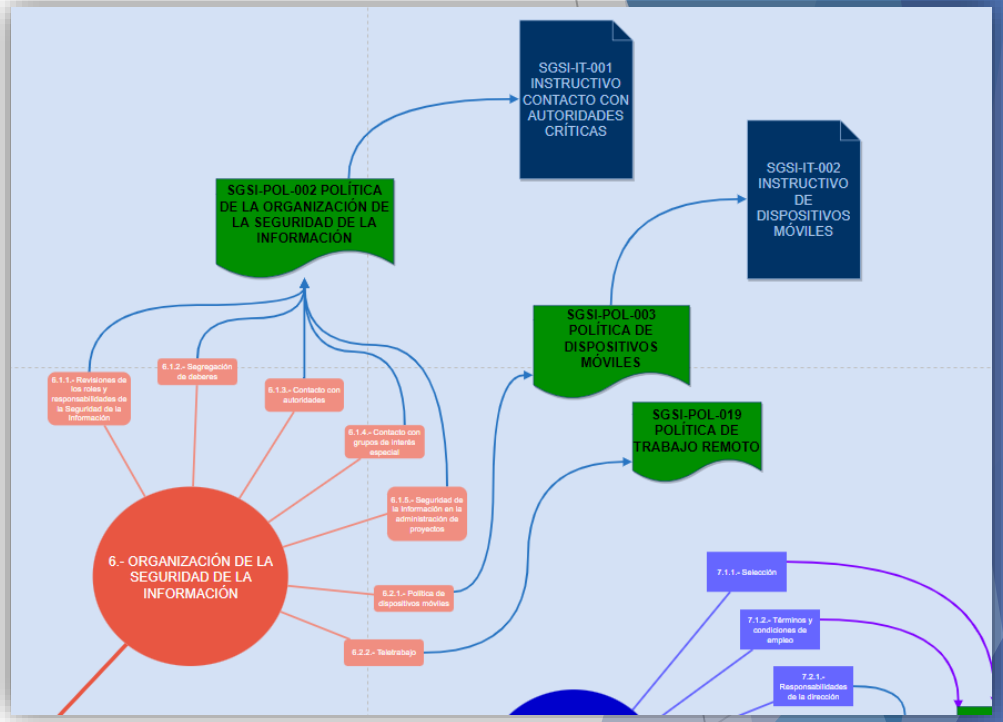
“Un sistema que determina que requiere protegerse, y por que , de que debe ser protegido y como protegerlo.”



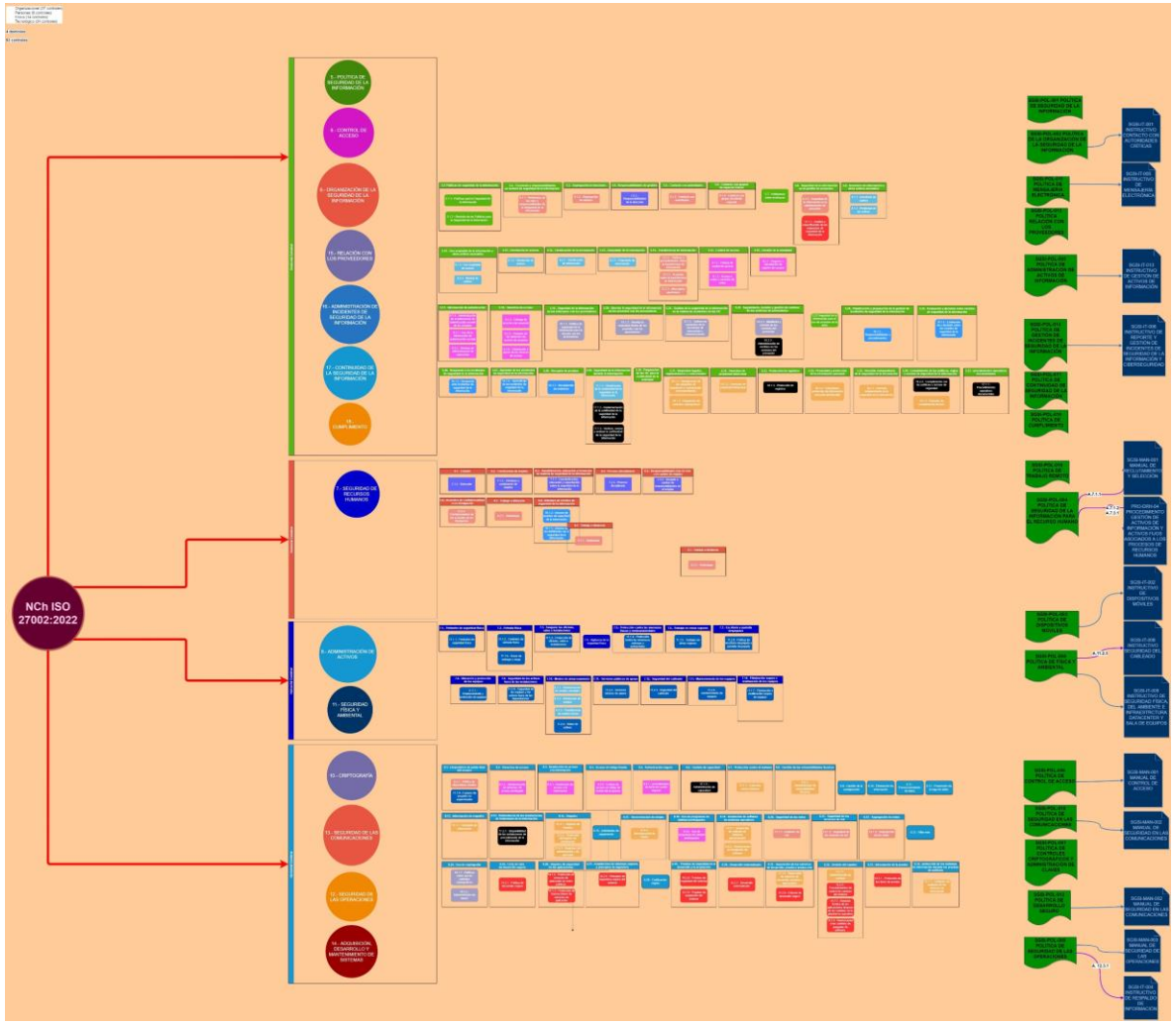
Fuente: managing information security risks, christopher albert 2003

Nuestra forma de enfrentarlo





Nuestra forma de enfrentarlo



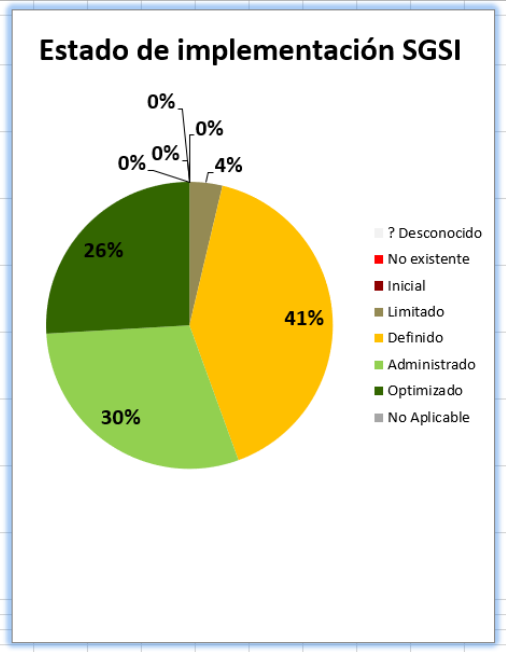
Organizacional (37 controles)
Personas (8 controles)
Físico (14 controles)
Tecnológico (34 controles)

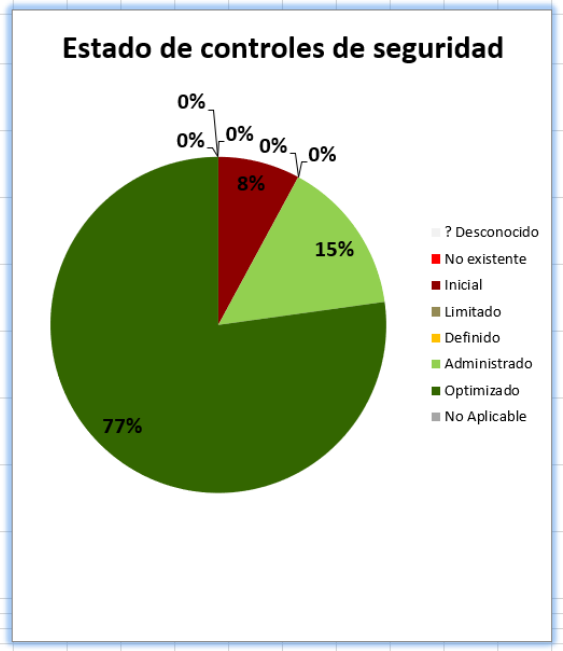
4 dominios

93 controles

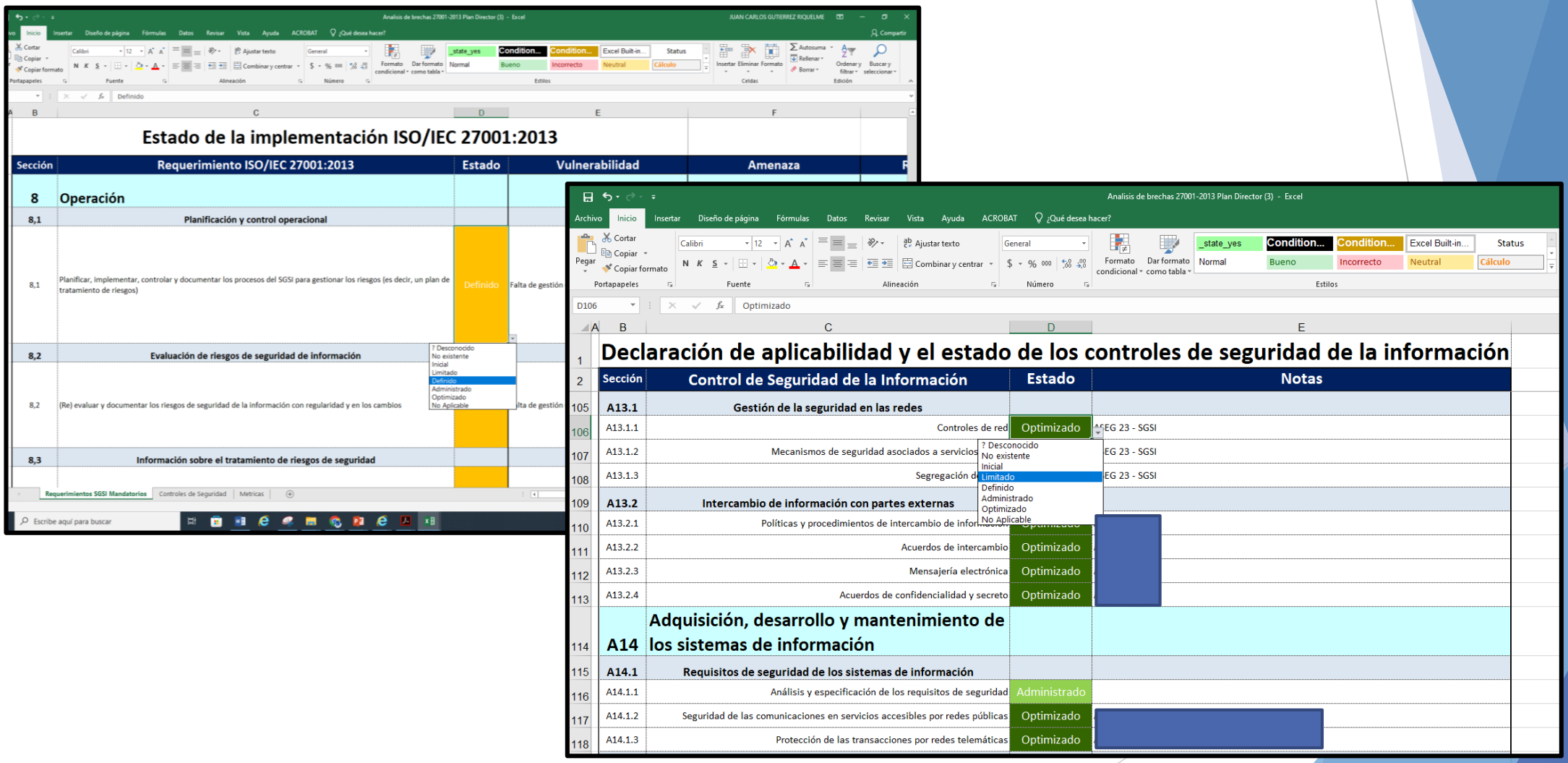
ANÁLISIS DE BRECHAS (GAP ANALISIS)

Estado	Significado	Procentaje de requisitos SGSI	de controles de la norma
? Desconocido	Aún no ha sido revisado	0%	0%
No existente	Ausencia total de política reconocible, procedimiento, de control, etc.	0%	0%
Inicial	El desarrollo apenas ha comenzado y requerirá un importante trabajo para cumplir con los requisitos	0%	8%
Limitado	Progresando muy bien, pero aún no ha concluido	4%	0%
Definido	El desarrollo es más o menos completo aunque existen detalles deficientes y / o que aún no se han implementado. Se cuenta con el apoyo activo de la alta dirección	41%	0%
Administrado	El desarrollo es completo, el proceso / control se ha aplicado y recientemente comenzó a operar	30%	15%
Optimizado	El requisito es plenamente satisfecho, está funcionando plenamente como era de esperar, se está supervisando activamente y mejorando, y hay evidencia sustancial para demostrar	26%	77%
No Aplicable	TODOS los requisitos en el cuerpo principal de la norma ISO / IEC 27001 son obligatorios si su SGSI quiere ser certificado. De lo contrario, se pueden ignorar ciertos controles	0%	0%
	Total	100%	100%





ANÁLISIS DE BRECHAS (GAP ANALISIS)



Estado de la implementación ISO/IEC 27001:2013

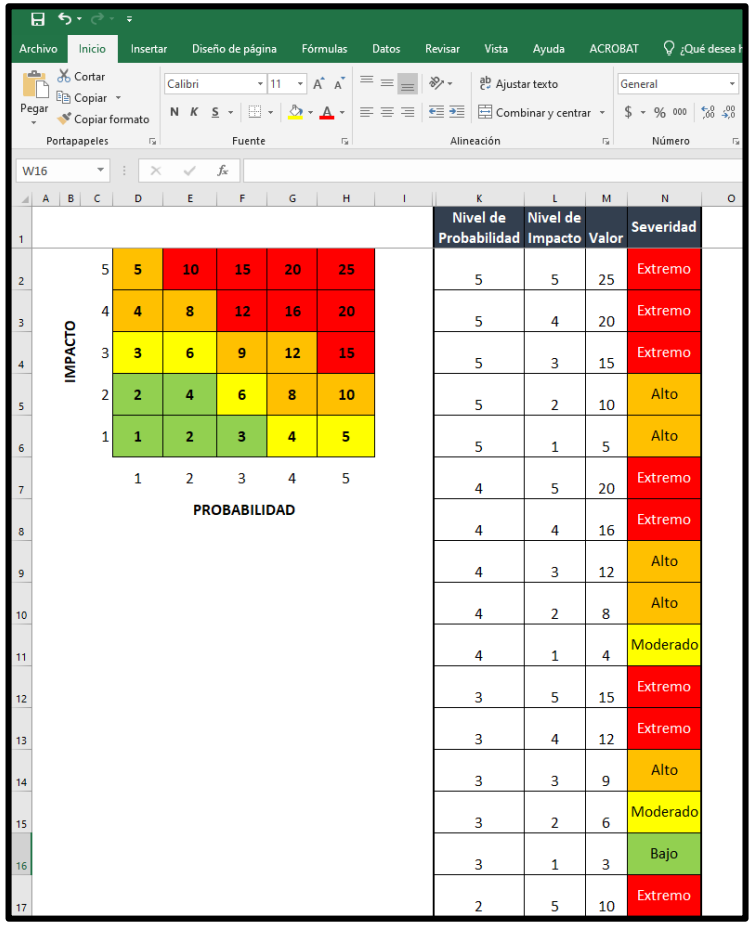
Sección	Requerimiento ISO/IEC 27001:2013	Estado	Vulnerabilidad	Amenaza
8	Operación			
8,1	Planificación y control operacional			
8,1	Planificar, implementar, controlar y documentar los procesos del SGSI para gestionar los riesgos (es decir, un plan de tratamiento de riesgos)	Definido	Falta de gestión	
8,2	Evaluación de riesgos de seguridad de información			
8,2	(Re) evaluar y documentar los riesgos de seguridad de la información con regularidad y en los cambios			
8,3	Información sobre el tratamiento de riesgos de seguridad			

? Desconocido
No existente
Inicial
Limitado
Definido
Administrado
Optimizado
No Aplicable

Declaración de aplicabilidad y el estado de los controles de seguridad de la información

Sección	Control de Seguridad de la Información	Estado	Notas
A13.1	Gestión de la seguridad en las redes		
A13.1.1	Controles de red	Optimizado	EG 23 - SGSI
A13.1.2	Mecanismos de seguridad asociados a servicios		EG 23 - SGSI
A13.1.3	Segregación d		EG 23 - SGSI
A13.2	Intercambio de información con partes externas		
A13.2.1	Políticas y procedimientos de intercambio de infor		
A13.2.2	Acuerdos de intercambio	Optimizado	
A13.2.3	Mensajería electrónica	Optimizado	
A13.2.4	Acuerdos de confidencialidad y secreto	Optimizado	
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información		
A14.1	Requisitos de seguridad de los sistemas de información		
A14.1.1	Análisis y especificación de los requisitos de seguridad	Administrado	
A14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Optimizado	
A14.1.3	Protección de las transacciones por redes telemáticas	Optimizado	

ANÁLISIS DE BRECHAS (GAP ANALISIS)



IMPACTO					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

PROBABILIDAD

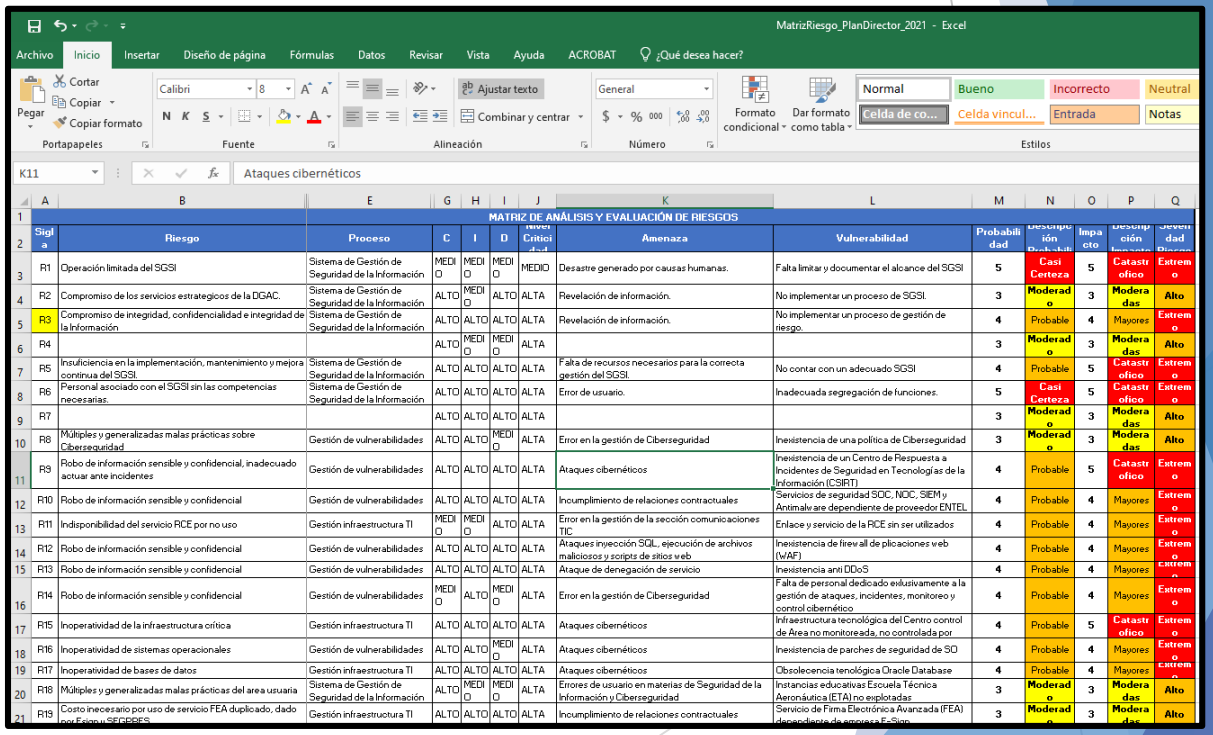
Nivel de Probabilidad	Nivel de Impacto	Valor	Severidad
5	5	25	Extremo
5	4	20	Extremo
5	3	15	Extremo
5	2	10	Alto
5	1	5	Alto
4	5	20	Extremo
4	4	16	Extremo
4	3	12	Alto
4	2	8	Alto
4	1	4	Moderado
3	5	15	Extremo
3	4	12	Extremo
3	3	9	Alto
3	2	6	Moderado
3	1	3	Bajo
2	5	10	Extremo

Valor	Categoría	Descripción
5	Catastrofico	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en la organización y/o comprometen totalmente la imagen de la organización.
4	Mayores	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en la organización y/o comprometen fuertemente la imagen de la organización.
3	Moderadas	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en ela organización y/o comprometen moderadamente la imagen de la organización
2	Menores	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en la organización y/o comprometen de forma menor la imagen de la organización
1	Insignificantes	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen de la organización.

Valor	Categoría	Descripción
5	Casi Certeza	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
4	Probable	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
3	Moderado	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
2	Improbable	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
1	Muy Improbable	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

ANÁLISIS DE BRECHAS (GAP ANALISIS)

Fuente de amenza	Motivación	Acciones de Amenaza
Hacker, cracker	Desafío	– Hacking
	Ego	– Ingeniería social
	Rebelión	– Intrusión de sistema/irrupciones
	Estatus	– Acceso no autorizado a sistema
	Dinero	
Delito informático	Destrucción de información	– Delito informático (por ejemplo, acoso cibernético)
	Divulgación ilegal de la información	– Acto fraudulento (por ejemplo, repetición, personifi cación, interceptación)
	Ganancia monetaria	– Soborno de información
	Alteración no autorizada de datos	– Engaño
		– Intrusión de sistemas
Terrorista	Chantaje	– Bomba
	Destrucción	– Guerra de información
	Explotación	– Ataque de sistema (por ejemplo, negación distribuida de servicio)
	Venganza	
	Ganancia política	– Penetración del sistema
	Cobertura mediática	– Manipulación del sistema
Espionaje industrial (inteligencia, compañías,Espionaje industrial(inteligencia, compañías,gobiernos extranjeros, otros intereses del gobierno)	Ventaja competitiva Espionaje económico	– Ventaja de defensa – Ventaja política – Explotación económica – Robo de información – Intrusión en privacidad personal – Ingeniería social – Penetración de sistema – Acceso no autorizado al sistema (acceso a información clasificada, propietaria, y/o relacionada con Tecnología)



Sigla	Riesgo	Proceso	C	I	D	Nivel Criticidad	Amenaza	Vulnerabilidad	Probabilidad	Descripción Probabilidad	Impacto	Descripción Impacto	Severidad Riesgo
R1	Operación limitada del SGSI	Sistema de Gestión de Seguridad de la Información	MEDIO	MEDIO	MEDIO	MEDIO	Desastre generado por causas humanas.	Falta limitar y documentar el alcance del SGSI	5	Casi Certeza	5	Catastrofico	Extremo
R2	Compromiso de los servicios estrategicos de la DGAC.	Sistema de Gestión de Seguridad de la Información	ALTO	MEDIO	ALTO	ALTA	Revelación de información.	No implementar un proceso de SGSI.	3	Moderado	3	Moderadas	Alto
R3	Compromiso de integridad, confidencialidad e integridad de la Información	Sistema de Gestión de Seguridad de la Información	ALTO	ALTO	ALTO	ALTA	Revelación de información.	No implementar un proceso de gestión de riesgo.	4	Probable	4	Mayores	Extremo
R4			ALTO	MEDIO	MEDIO	ALTA			3	Moderado	3	Moderadas	Alto
R5	Insuficiencia en la implementación, mantenimiento y mejora continua del SGSI.	Sistema de Gestión de Seguridad de la Información	ALTO	ALTO	ALTO	ALTA	Falta de recursos necesarios para la correcta gestión del SGSI.	No contar con un adecuado SGSI	4	Probable	5	Catastrofico	Extremo
R6	Personal asociado con el SGSI sin las competencias necesarias.	Sistema de Gestión de Seguridad de la Información	ALTO	ALTO	ALTO	ALTA	Error de usuario.	Inadecuada segregación de funciones.	5	Casi Certeza	5	Catastrofico	Extremo
R7			ALTO	ALTO	ALTO	ALTA			3	Moderado	3	Moderadas	Alto
R8	Múltiples y generalizadas malas prácticas sobre Ciberseguridad	Gestión de vulnerabilidades	ALTO	ALTO	MEDIO	ALTA	Error en la gestión de Ciberseguridad	Inexistencia de una política de Ciberseguridad	3	Moderado	3	Moderadas	Alto
R9	Robo de información sensible y confidencial, inadecuado actuar ante incidentes	Gestión de vulnerabilidades	ALTO	ALTO	ALTO	ALTA	Ataques cibernéticos	Inexistencia de un Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (CSIRT)	4	Probable	5	Catastrofico	Extremo
R10	Robo de información sensible y confidencial	Gestión de vulnerabilidades	ALTO	ALTO	ALTO	ALTA	Incumplimiento de relaciones contractuales	Servicios de seguridad SOC, NOC, SIEM y Antimalware dependiente de proveedor ENTEL	4	Probable	4	Mayores	Extremo
R11	Indisponibilidad del servicio RCE por no uso	Gestión infraestructura TI	MEDIO	MEDIO	ALTO	ALTA	Error en la gestión de la sección comunicaciones TIC	Enlace y servicio de la RCE sin ser utilizados	4	Probable	4	Mayores	Extremo
R12	Robo de información sensible y confidencial	Gestión de vulnerabilidades	ALTO	ALTO	ALTO	ALTA	Ataques inyección SQL, ejecución de archivos maliciosos y scripts de sitios web	Inexistencia de firevall de plicaciones web (WAF)	4	Probable	4	Mayores	Extremo
R13	Robo de información sensible y confidencial	Gestión de vulnerabilidades	ALTO	ALTO	ALTO	ALTA	Ataque de denegación de servicio	Inexistencia anti DDoS	4	Probable	4	Mayores	Extremo
R14	Robo de información sensible y confidencial	Gestión de vulnerabilidades	MEDIO	ALTO	MEDIO	ALTA	Error en la gestión de Ciberseguridad	Falta de personal dedicado exlusivamente a la gestión de ataques, incidentes, monitoreo y control cibernético	4	Probable	4	Mayores	Extremo
R15	Inoperatividad de la infraestructura crítica	Gestión infraestructura TI	ALTO	ALTO	ALTO	ALTA	Ataques cibernéticos	Infraestructura tecnológica del Centro control de Area no monitoreada, no controlada por	4	Probable	5	Catastrofico	Extremo
R16	Inoperatividad de sistemas operacionales	Gestión de vulnerabilidades	ALTO	ALTO	MEDIO	ALTA	Ataques cibernéticos	Inexistencia de parches de seguridad de SO	4	Probable	4	Mayores	Extremo
R17	Inoperatividad de bases de datos	Gestión infraestructura TI	ALTO	ALTO	ALTO	ALTA	Ataques cibernéticos	Obsolecencia tenológica Oracle Database	4	Probable	4	Mayores	Extremo
R18	Múltiples y generalizadas malas prácticas del area usuaria	Sistema de Gestión de Seguridad de la Información	ALTO	MEDIO	MEDIO	ALTA	Errores de usuario en materias de Seguridad de la Información y Ciberseguridad	Instancias educativas Escuela Técnica Aeronáutica (ETA) no esplotadas	3	Moderado	3	Moderadas	Alto
R19	Costo innecesario por uso de servicio FEA duplicado, dado por Esign y SEGPRES	Gestión infraestructura TI	ALTO	ALTO	ALTO	ALTA	Incumplimiento de relaciones contractuales	Servicio de Firma Electrónica Avanzada (FEA) dependiente de empresa E-Sign	3	Moderado	3	Moderadas	Alto

INVENTARIO DE ACTIVO

Nombre de la Institución: Dirección General de Aeronáutica Civil

	DESCRIPCIÓN DE PROCESOS			IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN											
Producto Estratégico	Proceso	Subproceso	Etapa relevante	Nombre Activo	Identificador o código	Tipo	Ubicación	Responsable / dueño	Soporte	Persona Autorizada para Manipular	Persona autorizada para Copiar	Medio de almacenamiento	Tiempo de retención	Disposición	Criterio de Busqueda
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Sistema de Gestion de Credenciales SCR	AVSEC002-015	Sistema		Director RR.HH / Director D.A.S.A.	Digital						
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Plataforma Sistema de Gestion de Credenciales SCR	AVSEC002-016	SW	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter.	Director TIC	Digital	Viviana Ros /Fernan					
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Plataforma Sistema de Gestion de Credenciales SCR	AVSEC002-017	SW	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter.	Director TIC	Digital	Viviana Ros /Fernan					
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Plataforma Sistema de Gestion de Credenciales SCR	AVSEC002-018	SW	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter.	Director TIC	Digital	Viviana Ros /Fernan					
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Plataforma Sistema de Gestion de Credenciales SCR	AVSEC002-019	SW	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter.	Director TIC	Digital	Responsable Subd Viviana Ros / Resp Fernando Sobarzo					
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Base de Datos SCR	AVSEC002-020	Base de Datos	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter.	Director TIC	Digital	Responsable Subd Viviana Ros / Resp Fernando Sobarzo					
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Sistema de Gestion de Credenciales SCR	AVSEC002-021	Infraestructura Física	Miguel Claro 1314, Providencia, Edifirio Aeronautico central, Piso -1, Datacenter. IBM X3650 M5, IBM V7000. Rack A02 y Rack A03								
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS	FTP-AVSEC-002: Credenciales Aeroportuarias Definitiva	Correo electronico adjunto R-AVSEC-012	AVSEC002-022	Documento			Digital						
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS		Solicitante credencial	AVSEC002-023	Persona			No Aplica						
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS		Funcionario AVSEC Supervisor de Turno	AVSEC002-024	Persona			No Aplica						
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	FTP-AVSEC-002: CREDENCIALES AEROPORTUARIAS		Funcionario AVSEC Jefe de Seguridad	AVSEC002-025	Persona			No Aplica						
SERVICIOS	SERVICIO DE SEGURIDAD DE	FTP-AVSEC-002:													

ANÁLISIS DE RIESGO POR ACTIVO

Nombre de la Institución: Dirección Nacional de Aeronáutica Civil

	CARACTERIZACIÓN DEL ACTIVO						MEDIDAS DE MITIGACION
Producto Estratégico	Proceso	Nombre Activo	Tipo	Descripción del Riesgo	Probabilidad de ocurrencia	Impacto	Severidad	Control para mitigar el riesgo
SERVICIOS AEREOPORTUARIOS	SERVICIO DE SEGURIDAD DE AVIACIÓN	Carta u Oficio avisa inicio de actividades	Documento	Pérdida o robo de Carta u Oficio, lo que genera la imposibilidad de operar el proceso	Improbable	Moderados	Moderado	A.8.1.1 A.8.1.2 A.8.1.3 A.8.1.4 A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.2 A.8.3.3 A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.5 A.11.1.6 A.11.2.9 A.12.4.1 A.16.1.1 A.16.1.2 A.16.1.3 A.17.1.1 A.17.1.2 A.17.1.3 A.18.1.3 A.18.1.4
				Falsificación de Carta u Oficio, lo que implica la obtención de credenciales no autorizadas	Improbable	Mayores	Alto	A.6.1.3 A.8.1.1 A.8.1.2 A.8.1.3 A.8.1.4 A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.2 A.8.3.3 A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.5 A.11.1.6 A.11.2.6 A.11.2.9 A.12.4.1 A.16.1.1 A.16.1.2 A.16.1.3 A.17.1.1 A.17.1.2 A.17.1.3 A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.2.1
								A.8.1.1

MATRIZ DE RIESGO POR PROCESO

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Producto Estratégico - Ficha A1	Proceso de Provisión	Activo	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad (Debilidad)	Descripción del Riesgo	Probabilidad	Impacto	Severidad	Tratamiento del riesgo	CONTROL	Nombre
		Documento papel - Expediente	RESERVADO	ALTA/MEDI	ALTA/MEDIA	Robo de medios o documentos.	Falta de control y capacitación en el traslado seguro de activos de	Fuga de información sensible, daño a la imagen institucional.	Improbable	Moderadas	Moderado	Reducir	A.08.03.0	Soportes físicos en tránsito
		Documento papel/digital - Informes y Certificados	PUBLICO	ALTA/MEDIA	ALTA/MEDIA	Error de uso de documento	Reglas de etiquetado no definidas	Adulteración, uso indebido de la información;	Improbable	Menores	Bajo	Reducir	A.08.02.02	Etiquetado y manipulado de la información
			RESERVADO			Error de uso de documento	Deficiente clasificación de los documentos	Adulteración, fuga, uso indebido de la información; Daño a la imagen institucional.	Moderado	Menores	Moderado	Reducir	A.08.02.01	Clasificación de la información
		Notebook Personal DGAC	PUBLICO	ALTA/MEDIA	ALTA/MEDIA	Salida no autorizada del equipo	Falta generar los registros de operación para el procedimiento para el control de activos fuera de las instalaciones de la institución	No disponibilidad del equipo	Muy Improbable	Moderadas	Moderado	Reducir	A.11.02.05	Salida de activos fuera de las dependencias de la empresa
						Robo, daño o pérdida del equipo;	Falta implemetar correctamente el procedimiento para el control de activos fuera de las instalaciones de la institución	Pérdida de información contenida en el equipo	Muy Improbable	Moderadas	Moderado	Reducir	A.11.02.06	Seguridad de los equipos y activos fuera de las instalaciones
		PC/Notebook Personal DGAC	PUBLICO	ALTA/MEDIA	ALTA/MEDIA	Eliminación indebida de la información contenida en el equipo	No se ha implementado correctamente el procedimiento de eliminación segura de información	Pérdida o adulteración de información contenida en el equipo	Muy Improbable	Mayores	Alto	Eliminar	A.11.02.07	Reutilización o retirada segura de dispositivos de almacenamiento
						Incorrecto uso de equipos	Falta revisar la correcta implementación del Procedimiento para la protección de equipos desatendidos.	Pérdida de información contenida en el equipo	Moderado	Moderadas	Alto	Eliminar	A.11.02.08	Equipo informático de usuario desatendido
		SISTEMAS DE APOYO A LOS PROCESOS DGAC	PUBLICO/RESERVADO	ALTA/MEDIA	ALTA/MEDIA	Acceso no autorizado	Falta revisar la correcta administración en la asignación y uso de derechos de acceso privilegiado	Adulteración del sistema	Muy Improbable	Moderadas	Moderado	Reducir	A.09.04.01	Restricción del acceso a la información
						Acceso no autorizado al sistema	Falta revisar el correcto cumplimiento del procedimiento de inicio seguro de sesión	Indisponibilidad de los sistemas	Improbable	Mayores	Alto	Eliminar	A.09.04.02	Procedimientos seguros de inicio de sesión
						Acceso no autorizado	Falta revisar la correcta administración en la asignación y uso de derechos de acceso privilegiado	Adulteración del sistema	Muy Improbable	Mayores	Alto	Eliminar	A.09.04.03	Gestión de contraseñas de usuario
						Falla del sistema	Falta implementar un procedimiento que regule el uso de programas utilitarios	Interrupción del normal desarrollo de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.09.04.04	Uso de programas utilitarios privilegiados
						Acceso indebido al código fuente	Falta revisar la correcta protección al código fuente del sistema	Adulteración del sistema	Muy Improbable	Moderadas	Moderado	Reducir	A.09.04.05	Control de acceso al código fuente de los programas
						Acceso no autorizado	No se ha definido formalmente qué información debe ser encriptada y no se han implementado controles criptográficos para protegerla	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Moderado	Moderadas	Alto	Eliminar	A.10.01.01	Política de uso de los controles criptográficos
						Acceso no autorizado	No se ha definido formalmente qué información debe ser encriptada y no se han implementado controles criptográficos para protegerla	Pérdida o adulteración de información contenida en el sistema.	Muy Improbable	Moderadas	Moderado	Reducir	A.10.01.02	Gestión de claves
						Mal funcionamiento o falla de los sistemas	Falta documentar todas las operaciones del sistema	Interrupción del normal desarrollo de los procesos de provisión institucionales	Improbable	Mayores	Alto	Eliminar	A.12.01.01	Documentación de procedimientos de operación
						Cambios no controlados en el sistema	Falta generar los registros de operación para el procedimiento que regula y controla los cambios realizados en los sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Improbable	Mayores	Alto	Eliminar	A.12.01.02	Gestión de cambios
						Acceso no autorizado al entorno operacinal	No está correctamente implementada la separación de ambientes es el ciclo de desarrollo del sistema	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.12.01.04	Separación de entornos de desarrollo, prueba y producción
						Falla del sistema	Falta generar los registros de operación para el procedimiento que registra y gestiona los eventos y fallas	Interrupción del normal desarrollo de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.12.04.01	Registro y gestión de eventos de actividad
						Adulteración de los registros del sistema.	Incorrecta protección y gestión de los registros del sistema	Incidentes de seguridad recurrentes	Muy Improbable	Moderadas	Moderado	Reducir	A.12.04.02	Protección de los registros de información
						Adulteración de los registros de actividades del operador y del administrador del sistema.	Falta proteger y gestionar de los registros del sistema	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.12.04.03	Registros de actividad del administrador y operador del sistema
						Inexistencia de una única fuente horaria para la sincronización de relojes de los sistemas	Los relojes de los sistemas existentes en la institución no están sincronizados	Incumplimiento de requisitos legales, normativos, contractuales, de cumplimiento con normas. Daño a la imagen institucional.	Muy Improbable	Mayores	Alto	Eliminar	A.12.04.04	Sincronización de relojes
						Sistema de información vulnerable	Falta la detección oportuna de vulnerabilidades técnicas del sistema	Interrupción del normal desarrollo de los procesos de provisión institucionales	Muy Improbable	Mayores	Alto	Eliminar	A.12.06.01	Gestión de las vulnerabilidades técnicas
						Falla del sistemas	Falta implementar un procedimiento de auditorías de sistemas que permita garantizar la operatividad continua de los sistemas	Interrupción del normal desarrollo de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.12.07.01	Controles de auditoría de los sistemas de información
						Deficiente seguridad en el desarrollo de los sistemas	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.14.01.01	Análisis y especificación de los requisitos de seguridad
						Acceso indebido o no autorizado.	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.14.01.02	Seguridad de las comunicaciones en servicios accesibles por redes públicas
						Acceso no autorizado	Falta revisar el correcto cumplimiento de las políticas y procedimeintos de redes y servicios de red	Pérdida o adulteración de información contenida en el sistema.	Muy Improbable	Moderadas	Moderado	Reducir	A.14.01.03	Protección de las transacciones por redes telemáticas
						Deficiente seguridad en el desarrollo de los sistemas	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.14.02.01	Política de desarrollo seguro de software
	FTP-AVSEC-001 CONTROL E INSPECCIÓN DE SEGURIDAD					Cambios fallidos, incorrectos y/o no controlados en los sistemas	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Improbable	Moderadas	Moderado	Reducir	A.14.02.02	Procedimientos de control de cambios en los sistemas
						Cambios fallidos, incorrectos y/o no controlados en los sistemas	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.14.02.03	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
						Cambios fallidos, incorrectos y/o no controlados en los sistemas	Falta definir e implementar los controles de desarrollo seguro de sistemas	Falla en los sistemas. Interrupción de los procesos de provisión institucionales	Muy Improbable	Moderadas	Moderado	Reducir	A.14.02.04	Restricciones a los cambios en los paquetes de software

¿ que es el nivel aceptable de riesgo ?

Debe ser el que nos permita mantener la CIA (confidencialidad, Integridad y Disponibilidad),de nuestros activos en el nivel establecido por nuestra organización enfocado principalmente en el apetito de riesgo definido.

Muchas Gracias

sgsi@dgac.gob.cl