# ELABORACION DE UN PLAN DE SEGURIDAD DE LA INFORMACION

## Postgrado en Gestión y Auditoria de la Seguridad

**AUTOR:** Ruth Aguilar Escobar

**CONSULTOR:** Arsenio tortajada gallego

**AREA DEL TRABAJO FINAL:** Sistema de Gestión de la Seguridad de la Información

**FECHA PRESENTACION:** 06/2017

# CONTENIDO

- OBJETIVO DEL PROYECTO
- JUSTIFICACION
- DESARROLLO DEL PROYECTO
- CONCLUSIONES

# OBJETIVO

Elaborar un plan director de seguridad de la Información de la Empresa A2

→ la guía corporativa para la implantación de las medidas de seguridad de la información y los sistemas de información

→ de la mano con los objetivos de la empresa

# NORMA DE REFERENCIA ISO/IEC 27001:2013

- Especifica los requisitos para establecer, implementar, mantener y mejorar de manera continua el sistema de gestión de la seguridad de la información dentro del contexto de una organización.

- Los requisitos son genéricos y son aplicables a todo tipo de organizaciones, independientemente tamaño o naturaleza.

- Es una norma certificable

# JUSTIFICACION

Los activos más importantes a proteger son:

- la información y
- los sistemas que manejan la información

→Es importante para las empresas garantizar un manejo seguro de la información.

# DESARROLLO DEL PROYECTO

Fase 1: Situación Actual

Fase 2: Sistema de Gestión Documental

Fase 3: Análisis de Riesgos

Fase 4: Propuestas de Proyectos

Fase 5: Auditoria de cumplimiento

Fase 6: Presentación de Resultados y entrega de Informes

# FASE 1: SITUACION ACTUAL

La empresa A2 es una empresa líder en la provisión de soluciones financieras y de pensiones

→El éxito comercial esta relacionado con la integridad y la confidencialidad

→ es de mucha importancia un manejo seguro de la información

# Contexto …

- Aplicaciones de contabilidad propias de la empresa.
- Aplicaciones para la gestión de recursos humanos
- Aplicaciones para la gestión de los productos (vida, vida empresas, vida independientes, grupo, pensión, saldo restante, …)

# Objetivos especificos del Plan

- Crear y promover la  cultura de seguridad dentro de la empresa
- Identificar el nivel de seguridad existente en los sistemas, servicios y aplicaciones
- Definir los roles, las responsabilidades en materia de seguridad
- Identificar los riesgos a los cuales están expuestos los activos de la empresa
- Definir los controles necesarios
- Definir y planificar los planes de acción a realizar
- Definir directrices en materia de la seguridad de la información
- Implantar y hacer un seguimiento  del plan de seguridad definido

→Garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de la información y los sistemas de información que maneja la empresa

# Estado actual de la seguridad

| Grupos de practicas del CMM | | | |
|---|---|---|---|
| **Nivel** | **%** | **Significado** | **Descripción** |
| N5 | 100% | Optimizado | Las prácticas de base están mejorando continuamente |
| N4 | 95% | Administrado | Las prácticas básicas son controladas cuantitativamente |
| N3 | 90% | Definido | Las prácticas básicas están bien definidas |
| N2 | 50% | Repetible | Las prácticas de base se planifican y rastrean |
| N1 | 10% | Inicial | Las prácticas básicas se realizan de manera informal |
| N0 | 0% | Ninguno | No existen practicas o procesos básicos. |

| Control | Cumplimento |
|---|---|
| 5 POLÍTICA DE SEGURIDAD | 50% |
| 6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | 46% |
| 7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS | 57% |
| 8. GESTIÓN DE ACTIVOS | 61% |
| 9. CONTROL DE ACCESOS | 65% |
| 10. CRIPTOGRAFÍA | 65% |
| 11. SEGURIDAD FÍSICA DEL ENTORNO | 72% |
| 12. SEGURIDAD DE LAS OPERACIONES | 68% |
| 13. SEGURIDAD DE LAS COMUNICACIONES | 58% |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN | 65% |
| 15. RELACIONES CON PROVEEDORES | 64% |
| 16 GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN | 64% |
| 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS | 68% |
| 18. CUMPLIMIENTO | 73% |
| NIVEL DE CUMPLIMIENTO GENERAL | 63% |

## % Cumplimiento de la norma ISO/IEC 27002:2013

# FASE 2: SISTEMA DE GESTION DOCUMENTAL SGSI

- Política de Seguridad
- Procedimiento de auditorias internas
- Gestión de Indicadores
- Declaración de aplicabilidad
- Procedimiento Revisión por la Dirección
- Gestión de Roles y Responsabilidades
- Metodología de análisis de Riesgo

# FASE 3: ANALISIS DE RIESGOS

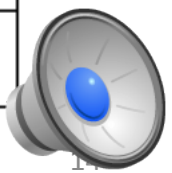
- Inventario de Activos
- Valoración de Activos
- Análisis de Amenazas
- Impacto potencial
- Impacto de Riesgo Aceptable y riesgo Residual

# INVENTARIO DE ACTIVOS

| Ámbitos de Clasificación |
|---|
| [D] Datos |
| [S] Servicios |
| [SW] Software |
| [HW] Hardware |
| [AUX] Equipamiento Auxiliar |
| [COM] Redes de comunicaciones |
| [I] Instalaciones |
| [P] Personal |

**[S] Software Aplicaciones Informáticas**

| ID | Nombre | Activo | Propietario |
|---|---|---|---|
| [SW.1] | CNS | Aplicación de gestión de datos clientes | Dirección operaciones |
| [SW.2] | EXX | Aplicación de gestión de acceso de usuarios a las distintas aplicaciones | Dirección operaciones |
| [SW.3] | XTR | Aplicación de gestión de los datos personales de los empleados de la empresa | Dirección RRHH |
| [SW.4] | BND | Aplicación de gestión de contratos de los clientes individuales | Dirección operaciones |
| [SW.5] | ULT | Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas | Dirección operaciones |



# INVENTARIO DE ACTIVOS

**[HW] Hardware**

| ID | Nombre | Activo | |
|---|---|---|---|
| [HW.1] | SFI | Servidor de aplicaciones internas/finanzas/admini/compta | Dirección IT |
| [HW.2] | SER | Servidores DNS | Dirección IT |
| [HW.3] | SDB | Servidores DB Oracle prod | Dirección IT |

| [D] Datos/Información | | | |
|---|---|---|---|
| **ID** | **Nombre** | **Activo** | |
| [D.1] | CFC | Código fuentes aplicaciones de gestión de contratos | Dirección operaciones |
| [D.2] | CFU | Código fuente aplicaciones de gestión de usuarios | Dirección Operaciones |
| [D.3] | CFE | Código fuente aplicaciones de gestión de datos de empleados | Dirección Operaciones |
| | | Código fuente aplicación de gestión de acceso de | Dirección |

# VALORACION DE ACTIVOS

| Dimensiones de valoración de activos |
|---|
| **[A] Autenticidad** |
| **[C] Confidencialidad de la información** |
| **[I] Integridad de la información** |
| **[D] Disponibilidad** |
| **[T] Trazabilidad** del uso del servicio |

| Valor | | | Criterio |
|---|---|---|---|
| 10 | E | Extremo | Daño Extremadamente Grave |
| 9 | MA | Muy Alto | Daño Muy Grave |
| 6-8 | A | Alto | Daño Grave |
| 3-5 | M | Medio | Daño Importante |
| 1-2 | MB | Bajo | Daño Menor |
| 0 | D | Despreciable | Irrelevante a efectos prácticos. |

# VALORACION DE ACTIVOS

**Tabla de activos con sus valoraciones**

SW

| ID | Activo | | Aspectos críticos | | | | |
|---|---|---|---|---|---|---|---|
| | | Valor | A | C | I | D | T |
| [SW.1] | Aplicación de gestión de datos clientes | MA | 9 | 9 | 9 | 9 | 9 |
| [SW.2] | Aplicación de gestión de acceso de usuarios a las distintas aplicaciones | MA | 8 | 8 | 8 | 9 | 9 |
| [SW.3] | Aplicación de gestión de los datos personales de los empleados de la empresa | MA | 8 | 8 | 8 | 9 | 8 |
| [SW.4] | Aplicación de gestión de contratos de los clientes individuales | MA | 8 | 8 | 8 | 8 | 8 |
| [SW.5] | Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas | MA | 9 | 9 | 9 | 9 | 9 |
| [SW.6] | Aplicación de gestión de contratos empresariales – seguros de grupo | MA | 9 | 9 | 9 | 9 | 9 |
| [SW.7] | Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos | MA | 8 | 8 | 8 | 9 | 8 |
| [SW.8] | Aplicación contable de la empresa | MA | 9 | 9 | 9 | 9 | 9 |
| [SW.9] | Servidor de documentos de desarrollo | M | 5 | 5 | 5 | 7 | 5 |
| [SW.10] | Servidor de documentos en TST | M | 7 | 7 | 7 | 7 | 7 |

# ANALISIS DE AMENAZAS

| Vulnerabilidad | ID | Rango | Valor |
|---|---|---|---|
| Frecuencia muy alta | MA | 1 vez al día | 1 |
| Frecuencia alta | A | 1 vez cada 2 semanas | 26/365 = 0.071 |
| Frecuencia media | M | 1 vez cada 2 meses | 6/365 = 0.016 |
| Frecuencia baja | B | 1 vez cada 6 meses | 2/365 = 0.005 |
| Frecuencia muy baja | MB | 1 vez al año | 1/365 = 0.002 |

| Impacto | ID | Valor |
|---|---|---|
| Muy alto | MA | 100% |
| Alto | A | 75% |
| Medio | M | 50% |
| Bajo | B | 20% |
| Muy Bajo | MB | 5% |

# ANALISIS DEVULNERABILIDADES Y AMENAZAS

**TABLA DE ANÁLISIS AMENAZAS/ACTIVOS**

| Grupo de Amenaza | Amenaza | Activo | Frecuencia/Amenaza | | Impacto Amenaza | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | ID | Valor | A | C | I | D | T |
| [N] Desastres naturales | | | | | | | | | |
| | [N.1] Fuego | | | | | | | | |
| | | [HW] Hardware | MB | 0,002 | | | | 100% | |
| | | [AUX] Equipo. Auxiliar | MB | 0,002 | | | | 100% | |
| | | [COM]: Redes | MB | 0,002 | | | | 100% | |
| | | [I] Instalaciones | MB | 0,002 | | | | 100% | |
| | | [P] Personal | MB | 0,002 | | | | 100% | |
| | [N.2] Daños por agua | | | | | | | | |
| | | [HW] Hardware | MB | 0,002 | | | | 75% | |
| | | [AUX] Equipo. Auxiliar | MB | 0,002 | | | | 75% | |
| | | [COM]: Redes | MB | 0,002 | | | | 75% | |
| | | [I] Instalaciones | MB | 0,002 | | | | 75% | |
| | [N.*] Desastres naturales | | | | | | | | |
| | | [SW] Software | MB | 0,002 | | | | 100% | |
| | | [HW] Hardware | MB | 0,002 | | | | 100% | |
| | | [AUX] Equipo. Auxiliar | MB | 0,002 | | | | 100% | |
| | | [I] Instalaciones | MB | 0,002 | | | | 100% | |
| | | | | | | | | | |
| [I] De origen industrial | | | | | | | | | |

# IMPACTO POTENCIAL

**IMPACTO POTENCIAL = VALOR DEL ACTIVO * VALOR DEL IMPACTO DE LA AMENAZA**

**VALORACION DEL IMPACTO POTENCIAL**

| ID | Activo | VALORACION | | | | | IMPACTO | | | | | IMPACTO POTENCIAL | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | C | I | D | T | A | C | I | D | T | A | C | I | D | T |
| [SW.1] | Aplicación de gestión de datos clientes | 9 | 9 | 9 | 9 | 9 | 75% | 75% | 75% | 100% | | 6,75 | 6,75 | 6,75 | 9 | 0 |
| [SW.2] | Aplicación de gestión de acceso de usuarios a las distintas aplicaciones | 8 | 8 | 8 | 9 | 9 | | | | | | 6 | 6 | 6 | 9 | 0 |
| [SW.3] | Aplicación de gestión de los datos personales de los empleados de la empresa | 8 | 8 | 8 | 9 | 8 | | | | | | 6 | 6 | 6 | 9 | 0 |
| [SW.4] | Aplicación de gestión de contratos de los clientes individuales | 8 | 8 | 8 | 8 | 8 | | | | | | 6 | 6 | 6 | 8 | 0 |
| [SW.5] | Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas | 9 | 9 | 9 | 9 | 9 | | | | | | 6,75 | 6,75 | 6,75 | 9 | 0 |
| [SW.6] | Aplicación de gestión de contratos empresariales – seguros de grupo | 9 | 9 | 9 | 9 | 9 | | | | | | 6,75 | 6,75 | 6,75 | 9 | 0 |

# NIVEL DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

**RIESGO= IMPACTO POTENCIAL * FRECUENCIA**

| Escalas | | |
|---|---|---|
| Impacto | Frecuencia | Riesgo |
| MA: muy alto | MA: prácticamente seguro | MA: crítico |
| A: alto | A: probable | A: importante |
| M: medio | M: posible | M: apreciable |
| B: bajo | B: poco probable | B: bajo |
| MB: muy bajo | MB: muy raro | MB: despreciable |

| | RIESGO | PROBABILIDAD | | | | |
|---|---|---|---|---|---|---|
| | | MB (0,002) | B (0,005) | M (0,016) | A (0,071) | MA (1) |
| IMPACTO | MA (10) | A | MA | MA | MA | MA |
| | A (7-9) | M | A | A | MA | MA |
| | M (4-6) | B | M | M | A | A |
| | B (2-3) | MB | B | B | M | M |
| | MB (1) | MB | MB | MB | B | B |

UOC Universitat Oberta de Catalunya www.uoc.edu · UAB Universitat Autònoma de Barcelona · Universitat Rovira i Virgili · UIB Universitat de les Illes Balears

## TABLA DE VALORACION DE RIESGO

| Tipo | Activo | Valor | Freq. | IMPACTO POTENCIAL | | | | | RIESGO | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | A | C | I | D | T | A | C | I | D | T |
| [SW.1] | Aplicación de gestión de datos clientes | M | 0,016 | 6,75 | 6,75 | 6,75 | 9 | 0 | 0,11 | 0,11 | 0,11 | 0,14 | 0 |
| [SW.2] | Aplicación de gestión de acceso de usuarios a las distintas aplicaciones | | | 6 | 6 | 6 | 9 | 0 | 0,10 | 0,10 | 0,10 | 0,14 | 0 |
| [SW.3] | Aplicación de gestión de los datos personales de los empleados de la empresa | | | 6 | 6 | 6 | 9 | 0 | 0,10 | 0,10 | 0,10 | 0,14 | 0 |
| [SW.4] | Aplicación de gestión de contratos de los clientes individuales | | | 6 | 6 | 6 | 8 | 0 | 0,10 | 0,10 | 0,10 | 0,13 | 0 |
| [SW.5] | Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas | | | 6,75 | 6,75 | 6,75 | 9 | 0 | 0,11 | 0,11 | 0,11 | 0,14 | 0 |
| [SW.6] | Aplicación de gestión de contratos empresariales – seguros de grupo | | | 6,75 | 6,75 | 6,75 | 9 | 0 | 0,11 | 0,11 | 0,11 | 0,14 | 0 |
| [SW.7] | Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos | | | 6 | 6 | 6 | 9 | 0 | 0,10 | 0,10 | 0,10 | 0,14 | 0 |
| [SW.8] | Aplicación contable de la empresa | | | 6,75 | 6,75 | 6,75 | 9 | 0 | 0,11 | 0,11 | 0,11 | 0,14 | 0 |
| [I.9] | Espacio de almacenamiento de documentos papel seguros | | | 0 | 0 | 0 | 8 | 0 | 0 | 0 | 0 | 0,13 | 0 |
| [D.1] | Código fuentes aplicaciones de gestión de contratos | M | 0,016 | 9 | 10 | 10 | 10 | 9 | 0,14 | 0,16 | 0,16 | 0,16 | 0,14 |
| [D.2] | Código fuente aplicaciones de gestión de usuarios | | | 9 | 10 | 10 | 10 | 9 | 0,14 | 0,16 | 0,16 | 0,16 | 0,14 |
| [D.3] | Código fuente aplicaciones de gestión de datos de empleados | | | 9 | 10 | 10 | 10 | 9 | 0,14 | 0,16 | 0,16 | 0,16 | 0,14 |
| [D.4] | Código fuente aplicación de gestión de acceso de usuarios / aplicaciones | | | 9 | 10 | 10 | 10 | 9 | 0,14 | 0,16 | 0,16 | 0,16 | 0,14 |
| [D.5] | Datos de clientes individuales | | | 9 | 10 | 9 | 9 | 8 | 0,14 | 0,16 | 0,14 | 0,14 | 0,13 |
| [D.6] | Datos de clientes empresariales | | | 9 | 10 | 9 | 9 | 8 | 0,14 | 0,16 | 0,14 | 0,14 | 0,13 |
| [D.7] | Datos de clientes independientes | | | 9 | 10 | 9 | 9 | 8 | 0,14 | 0,16 | 0,14 | 0,14 | 0,13 |
| [D.8] | Datos de los empleados de la empresa | | | 8 | 10 | 9 | 7 | 8 | 0,13 | 0,16 | 0,14 | 0,11 | 0,13 |
| [D.9] | Datos de acceso a las aplicaciones (roles y responsabilidades) | | | 8 | 9 | 8 | 9 | 9 | 0,13 | 0,14 | 0,13 | 0,14 | 0,14 |
| [D.10] | Documentos de clientes | | | 8 | 8 | 8 | 9 | 8 | 0,13 | 0,13 | 0,13 | 0,14 | 0,13 |
| [D.11] | Documentos de empleados | | | 8 | 8 | 8 | 9 | 8 | 0,13 | 0,13 | 0,13 | 0,14 | 0,13 |
| [D.12] | Documentos otros | | | 5 | 6 | 7 | 7 | 8 | 0,08 | 0,10 | 0,11 | 0,11 | |
| [D.13] | Datos de soporte y licencias | | | 5 | 6 | 7 | 7 | 8 | 0,08 | 0,10 | 0,11 | 0,11 | |
| [D.14] | Log de servidores y log de clientes | | | 9 | 10 | 10 | 10 | 9 | 0,14 | 0,16 | 0,16 | 0,1 | |

# IMPACTO DE RIESGO ACEPTABLE Y RIESGO RESIDUAL

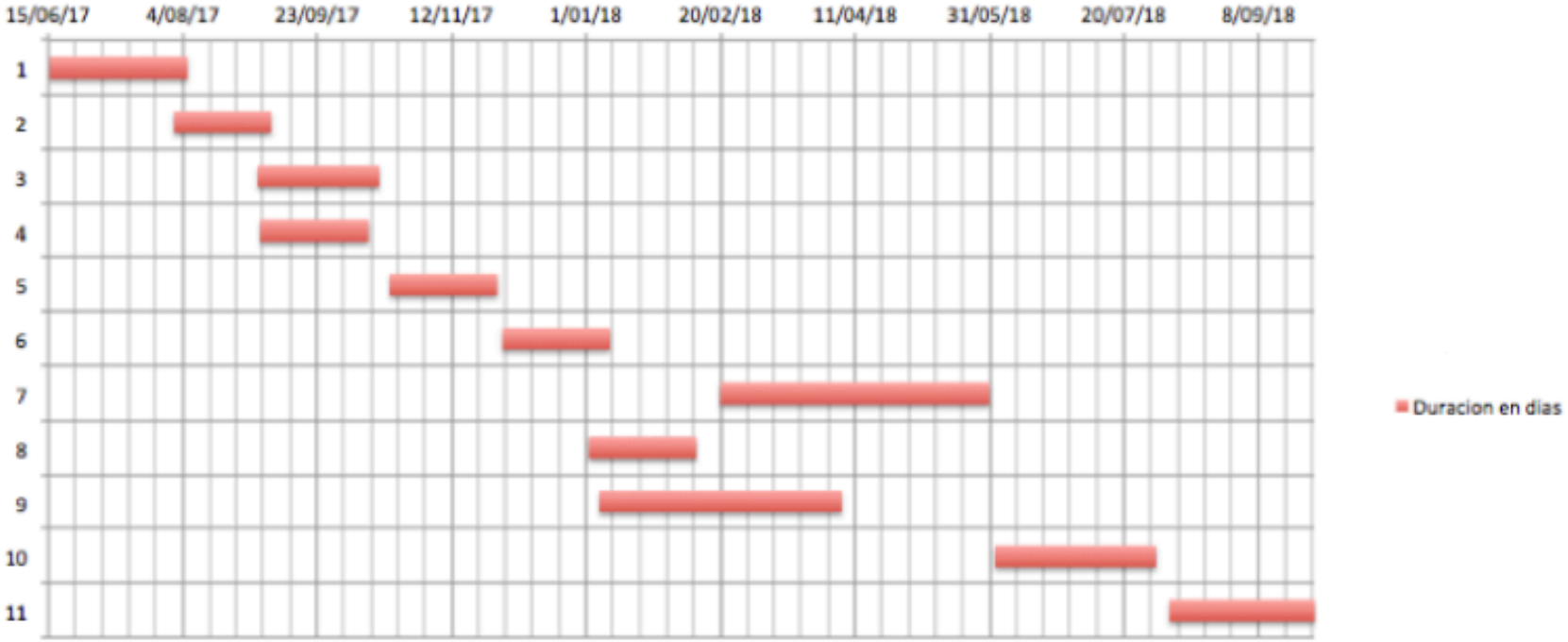
| ID | Activo | Riesgo |
|---|---|---|
| [D.1] | Código fuentes aplicaciones de gestión de contratos | MA |
| [D.2] | Código fuente aplicaciones de gestión de usuarios | |
| [D.3] | Código fuente aplicaciones de gestión de datos de empleados | |
| [D.4] | Código fuente aplicación de gestión de acceso de usuarios / aplicaciones | |
| [D.14] | Log de servidores y log de clientes | |
| [D.5] | Datos de clientes individuales | |
| [D.6] | Datos de clientes empresariales | |

| ID | Activo | Riesgo |
|---|---|---|
| [SW.1] | Aplicación de gestión de datos clientes | |
| [SW.2] | Aplicación de gestión de acceso de usuarios a las distintas aplicaciones | |
| [SW.3] | Aplicación de gestión de los datos personales de los empleados de la empresa | |
| [SW.4] | Aplicación de gestión de contratos de los clientes individuales | |
| [SW.5] | Aplicación de gestión de contratos de los clientes independientes y pequeñas empresas | |
| [SW.6] | Aplicación de gestión de contratos empresariales – seguros de grupo | |
| [SW.7] | Aplicación de gestión de los ingresos y egresos de la empresa por concepto de la gestión de los contratos | |

# FASE 4: PROPUESTAS DE PROYECTOS

| ID | Nombre | Plazos |
|---|---|---|
| **PR001** | Políticas de seguridad de la Información | **A corto plazo** |
| **PR001** | Plan de Continuidad del Negocio | |
| **PR003** | Plan de Formación y concientización | |
| **PR004** | Políticas de control de acceso y de acceso a la red y los servicios de red | |
| **PR005** | Gestión del acceso del usuario | |
| **PR002** | Plan de continuidad del Negocio | **A mediano Plazo** |
| **PR006** | Control de acceso al sistema y aplicaciones | |
| **PR007** | Revisión del SGSI | |
| **PR008** | Mejora en la gestión de Recursos Humanos | **A largo plazo** |
| **PR009** | 2F autenticación | |
| **PR010** | Clasificación de la Información | |
| **PR011** | Copias de Respaldo | |

# FASE 4: PROPUESTAS DE PROYECTOS

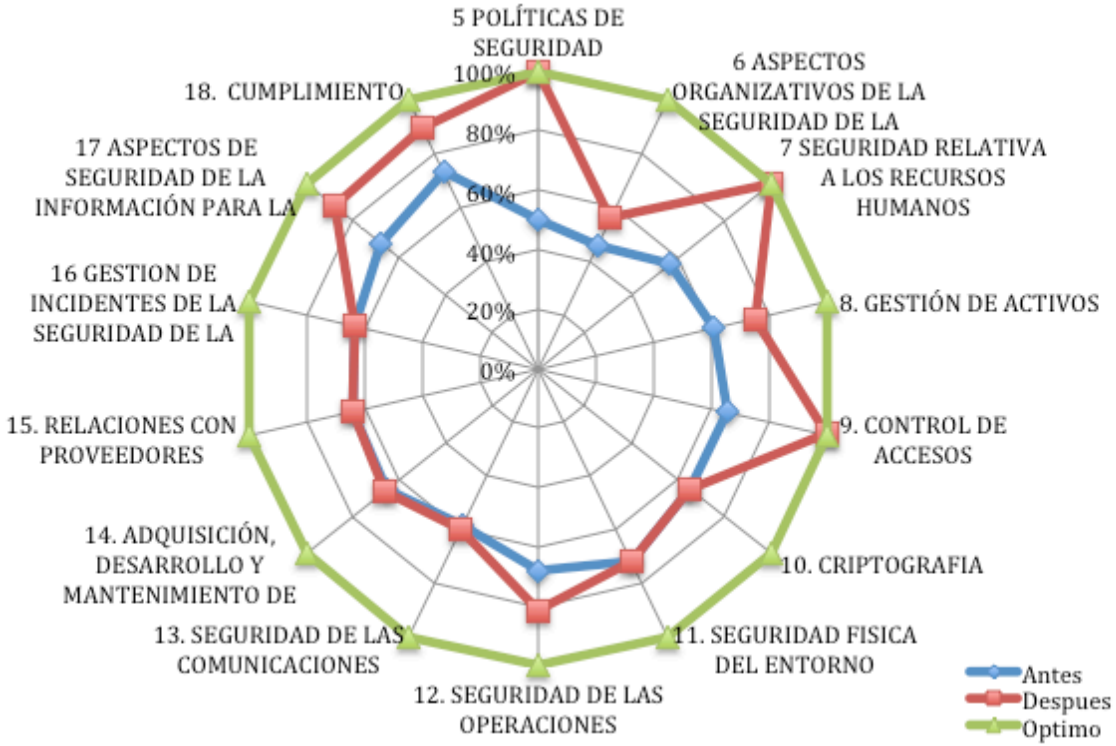


| Id del proyecto | PR001 |
|---|---|
| Nombre del proyecto | Políticas de seguridad de la Información |
| Objetivo | Actualizar el documento de políticas de seguridad.<br>Mejorar el soporte de la gestión de la seguridad de la información. |
| Responsable | Responsable de la seguridad |
| Descripción | Este proyecto busca actualizar las políticas existentes dentro de la organización en función a los cambios tecnológicos, cambios en la empresa y/o nuevos requerimientos no tratados y necesidades en materia de seguridad.<br>Se busca identificar políticas obsoletas, actualizar y definir nuevas políticas necesarias para el manejo seguro de la información en las condiciones actuales de la organización.<br>Este documento debe ser aprobado por la dirección.<br>Este documento debe ser implantado inmediatamente.<br>Este documento debe ser revisado anualmente. |
| Activos Afectados | Todos los activos |
| Dominios ISO/IEC 27002:2013 | A.5 |
| Dimensiones de seguridad afectadas | ACIDT |
| Riesgos mitigados | Autenticación, Confidencialidad, Integridad, Disponibilidad y trazabilidad de la información. |
| Duración | 40 días |
| Recursos | Responsable de la Seguridad<br>Director General<br>Directivos de la empresa<br>Propietarios de la Información y los Sistemas |
| Costos Estimados | €20000.- |

# CUMPLIMIENTO DESPUES DE LA IMPLEMENTACION DE PROYECTOS

| Dominio | Antes | Después |
|---|---|---|
| 5 POLÍTICAS DE SEGURIDAD | 50% | 100% |
| 6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | 46% | 56% |
| 7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS | 57% | 100% |
| 8. GESTIÓN DE ACTIVOS | 61% | 75% |
| 9. CONTROL DE ACCESOS | 65% | 100% |
| 10. CRIPTOGRAFIA | 65% | 65% |
| 11. SEGURIDAD FISICA DEL ENTORNO | 72% | 72% |
| 12. SEGURIDAD DE LAS OPERACIONES | 68% | 81% |
| 13. SEGURIDAD DE LAS COMUNICACIONES | 58% | 60% |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI | 65% | 66% |
| 15. RELACIONES CON PROVEEDORES | 64% | 64% |
| 16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION | 64% | 64% |
| 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS | 68% | 88% |
| 18. CUMPLIMIENTO | 73% | 90% |
| **CUMPLIMIENTO GENERAL** | **63%** | **77%** |

# EVOLUCION DE LOS DOMINIOS



# FASE 5: AUDITORIA DE CUMPLIMIENTO

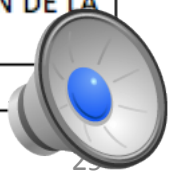
Se evalúa el nivel de cumplimiento con las buenas prácticas en materia de seguridad.

Marco de referencia → ISO/IEC 27002:2013

11 dominios y

114 objetivos de control

| Dominios |
|---|
| 5 POLÍTICAS DE SEGURIDAD |
| 6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN |
| 7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS |
| 8. GESTIÓN DE ACTIVOS |
| 9. CONTROL DE ACCESOS |
| 10. CRIPTOGRAFIA |
| 11. SEGURIDAD FISICA DEL ENTORNO |
| 12. SEGURIDAD DE LAS OPERACIONES |
| 13. SEGURIDAD DE LAS COMUNICACIONES |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI |
| 15. RELACIONES CON PROVEEDORES |
| 16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION |
| 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS |
| 18. CUMPLIMIENTO |



# Metodologia

- Evaluación al cumplimiento de cada uno de los controles de la norma ISO / IEC 27002: 2013 utilizando Modelo de Madurez de la Capacidad (CMM).

## FASES

- Fase 1: Recolección de la Información
- Fase 2: Ejecución de pruebas documentadas
- Fase3: Análisis de la información

  → a partir de este análisis que se puede concluir la efectividad de los controles implementados.

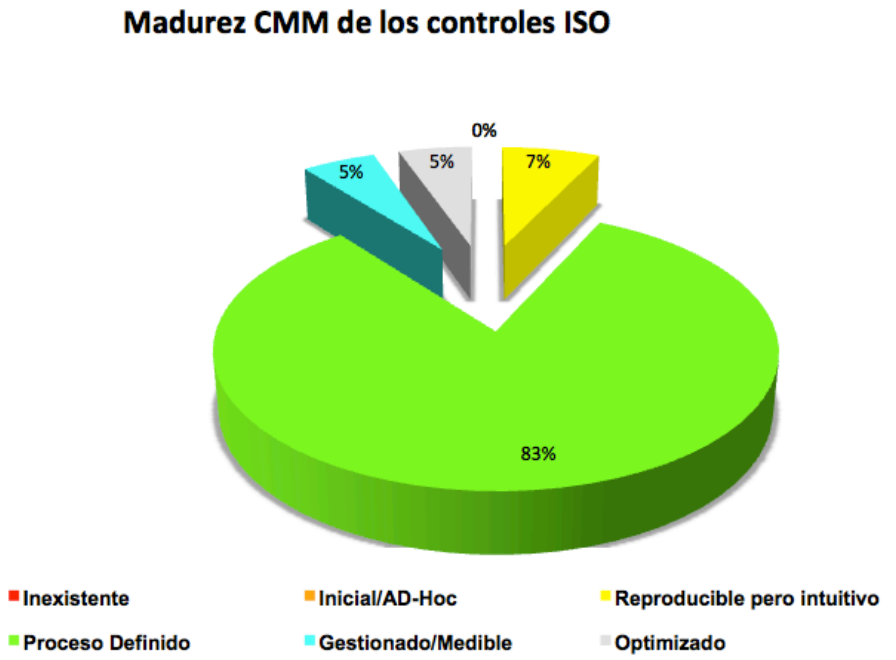
- Fase 4: Elaboración y presentación del Reporte de la Auditoria

# FASE 5: AUDITORIA DE CUMPLIMIENTO

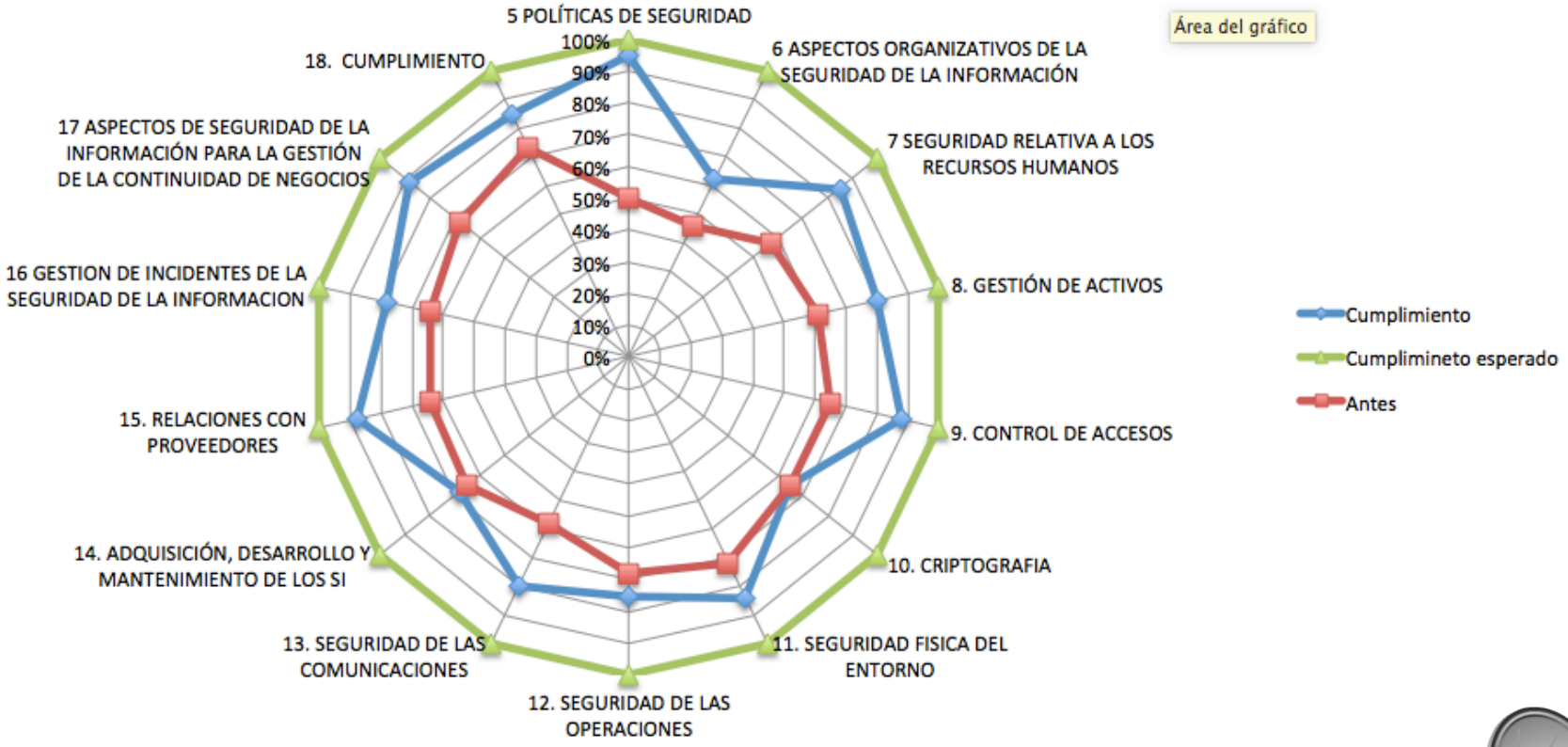
| Efectividad | CMM | Significado | Descripción |
|---|---|---|---|
| 0% | L0 | Inexistente | Carencia completa de cualquier proceso reconocible.<br>No se ha reconocido siquiera que existe un problema a resolver. |
| 10% | L1 | Inicial/AD-hoc | Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal.<br>Los procedimientos son inexistentes o localizados en áreas concretas.<br>No existen plantillas definidas a nivel corporativo. |
| 50% | L2 | Reproducible, pero intuitivo | Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea.<br>Se normalizan las buenas prácticas en base a la experiencia y al método.<br>No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.<br>Se depende del grado de conocimiento de cada individuo. |
| 90% | L3 | Proceso definido | La organización entera participa en el proceso.<br>Los procesos están implantados, documentados y comunicados mediante entrenamiento. |
| 95% | L4 | Gestionado y medible | Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.<br>Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. |
| 100% | L5 | Optimizado | Los procesos están bajo constante mejora.<br>En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos. |

# FASE 5: AUDITORIA DE CUMPLIMIENTO

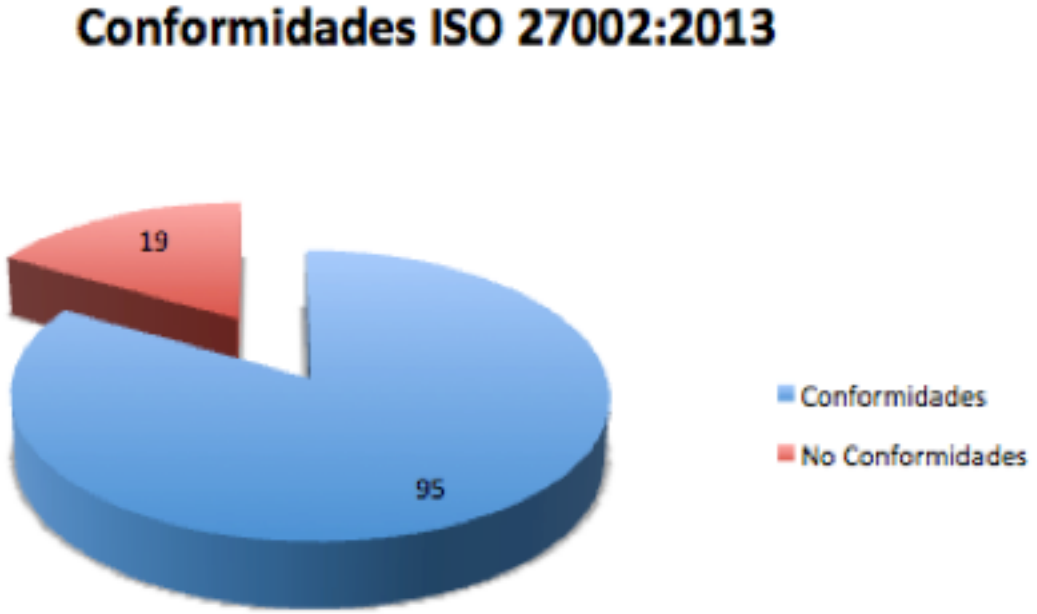
| Nivel de Madurez | No Controles |
|---|---|
| Inexistente | 0 |
| Inicial/AD-Hoc | 0 |
| Reproducible pero intuitivo | 8 |
| Proceso Definido | 94 |
| Gestionado/Medible | 6 |
| Optimizado | 6 |
| Total | 114 |



# FASE 5: AUDITORIA DE CUMPLIMIENTO



# FASE 5: AUDITORIA DE CUMPLIMIENTO



| Dominios | Mayores | Menores |
|---|---|---|
| 5 POLÍTICAS DE SEGURIDAD | | |
| 6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | | 3 |
| 7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS | | |
| 8. GESTIÓN DE ACTIVOS | | |
| 9. CONTROL DE ACCESOS | 3 | |
| 10. CRIPTOGRAFIA | | 1 |
| 11. SEGURIDAD FISICA DEL ENTORNO | | 2 |
| 12. SEGURIDAD DE LAS OPERACIONES | | 4 |
| 13. SEGURIDAD DE LAS COMUNICACIONES | | |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI | | 4 |
| 15. RELACIONES CON PROVEEDORES | | |
| 16 GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION | | 1 |
| 17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS | | |
| 18. CUMPLIMIENTO | | 1 |
| | 3 | 16 |

# FASE 5: AUDITORIA DE CUMPLIMIENTO

# INFORME DE AUDITORIA

- Objetivo
- Alcance
- Metodología
- Hallazgos
  - No conformidades
  - Punto fuertes
  - Oportunidades de mejora

| ID: NC-002 | Fecha: | 20/05/2017 |
|---|---|---|
| **Descripción NC** | | |
| - Existen registros de un numero importante de incidentes de seguridad en los dispositivos móviles.<br>- Existen registros de un numero importante de incidentes de Seguridad durante el teletrabajo. | | |
| **Tipo** | ☐ **Mayor** | ☑ **Menor** |
| **Referencia normativa** | ISO / IEC 27002 | |
| **Controles** | | **Dominio** |
| 6.3.1 Política de uso de dispositivos para movilidad.<br>6.1.2 Teletrabajo | | 6.2 Dispositivos para movilidad y teletrabajo |
| **Acción Correctora** | | |
| -Organizar sesiones de formación y concientización sobre la seguridad de la información y los riesgos en general y en particular en lo que se refiere a los dispositivos móviles y el teletrabajo.<br>- Cada empleado que utilice un dispositivo móvil y/o trabaje a distancia debe pasar esta formación/sesión antes de usar un dispositivo móvil o comenzar el teletrabajo.<br>-Cada empleado debe firmar un documento de responsabilidad. | | |
| **Responsable Ejecución acción correctora** | | |
| Responsable de Recursos Humanos – Responsable de la Seguridad | | 0 |

# FASE 6 : PRESENTACION DE RESULTADOS

- Memoria
- Informe Ejecutivo
- Presentacion (video)

# CONCLUSIONES DEL PROYECTO

- La implementación de un Plan de Seguridad de la Información es un proceso continuo
- La implementación de este plan ha mejorado el nivel de seguridad de la información en la empresa.
- Requiere de la participación y del compromiso de todos los miembros del personal y principalmente de la Dirección.
- Se ha creado una estructura interna con responsabilidad directa sobre la seguridad de la información. Se han definido los roles y las responsabilidades.
- Este plan constituye la única guía corporativa que implementa de las medidas de seguridad de la información y los sistemas de información dentro de la organización.
- El proceso de formación/concientización es fundamental para la evolución exitosa de este plan. Si bien se ha logrado mejorar los niveles de concientización del personal, se recomienda que el proceso de formación sea continua