**MANUAL DEL SISTEMA DE GESTIÓN INTEGRADO**



|  |  |  |
| --- | --- | --- |
| ***REVISION*** | ***FECHA*** | ***MODIFICACIÓN*** |
| 0 | 13/08/2014 | Elaboración Inicial del Manual |
| 1 | 30/01/2015 | Revisión y aprobación |
| 2 | 12/02/2015 | Revisión y aprobación |
| 3 | 19/02/2015 | Revisión y aprobación |
| 4 | 20/11/2015 | Revisión y aprobación |
| 5 | 17/11/2016 | Revisión y aprobación |
| 6 | 20/06/2017 | Revisión y adaptación a la nueva norma |
| 7 | 18/12/2017 | Revisión y aprobación del manual |
| 8 | 11/2018 | Revisión y aprobación del manual |
| 9 | 02/2019 | Revisión y aprobación del manual |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| Elaborado/Revisado por:  Resp. Gestión de la Calidad | Aprobado por:  Director Gerente | Copia controlada Copia no controlada |
| Fecha: Feb 2019 | Fecha: Feb 2019 | Número de copia: 1 |

Contenido

[1. INTRODUCCIÓN: 3](#_Toc2078700)

[1.1. PRESENTACIÓN: 3](#_Toc2078701)

[1.2. CONTROL DE REVISIONES DEL MANUAL DE CALIDAD 3](#_Toc2078702)

[1.2.1. Preparación, actualización y distribución. 4](#_Toc2078703)

[1.2.2. Copias Controladas: 4](#_Toc2078704)

[1.3. POLÍTICA DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN 4](#_Toc2078705)

[1.3.1. Declaración de la política de Calidad y Seguridad de la Información. 4](#_Toc2078706)

[2. OBJETO Y CAMPO DE APLICACIÓN. 6](#_Toc2078707)

[3. REFERENCIAS NORMATIVAS. 7](#_Toc2078708)

[4. TÉRMINOS Y DEFINICIONES. 7](#_Toc2078709)

[5. CONTEXTO DE LA ORGANIZACIÓN. 8](#_Toc2078710)

[5.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO. 8](#_Toc2078711)

[5.2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS. 10](#_Toc2078712)

[5.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN 10](#_Toc2078714)

[5.4. SISTEMA DE GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y SUS PROCESOS 11](#_Toc2078715)

[6. LIDERAZGO. 12](#_Toc2078716)

[6.1. LIDERAZGO Y COMPROMISO. 12](#_Toc2078717)

[6.1.1. LIDERAZGO Y COMPROMISO PARA EL SISTEMA DE GESTIÓN DE CALIDAD. 12](#_Toc2078718)

[6.1.2. ENFOQUE AL CLIENTE. 12](#_Toc2078719)

[*6.2.* *POLÍTICA DE CALIDAD.* 13](#_Toc2078720)

[6.3. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN. 13](#_Toc2078721)

[7. PLANIFICACIÓN. 14](#_Toc2078722)

[7.1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES. 14](#_Toc2078723)

[7.2. OBJETIVOS DE LA CALIDAD, SEGURIDAD Y PLANIFICACIÓN PARA LOGRARLOS. 15](#_Toc2078724)

[7.3. PLANIFICACIÓN DE LOS CAMBIOS. 15](#_Toc2078725)

[8. SOPORTE 16](#_Toc2078726)

[8.1. RECURSOS 16](#_Toc2078727)

[8.1.1. PERSONAS 16](#_Toc2078728)

[*8.1.2.* INFRAESTRUCTURA*.* 16](#_Toc2078729)

[8.1.3. AMBIENTE PARA LA OPERACIÓN DE LOS PROCESOS. 16](#_Toc2078730)

[8.1.4. RECURSOS DE SEGUIMIENTO Y MEDICIÓN. 17](#_Toc2078731)

[8.1.5. CONOCIMIENTOS DE LA ORGANIZACIÓN. 17](#_Toc2078732)

[8.2. COMPETENCIA. 17](#_Toc2078733)

[8.3. COMPETENCIA, TOMA DE CONCIENCIA Y FORMACIÓN 17](#_Toc2078734)

[*8.4.* COMUNICACIÓN*.* 18](#_Toc2078735)

[8.5. INFORMACIÓN DOCUMENTADA. 18](#_Toc2078736)

[8.5.1. GENERALIDADES. 18](#_Toc2078737)

[8.5.2. CREACIÓN Y ACTUALIZACIÓN. 19](#_Toc2078738)

[8.5.3. CONTROL DE LA INFORMACIÓN DOCUMENTADA. 19](#_Toc2078739)

[9. OPERACIÓN. 20](#_Toc2078740)

[9.1. PLANIFICACIÓN Y CONTROL OPERACIONAL: 20](#_Toc2078741)

[9.2. DETERMINACIÓN DE LOS REQUISITOS PARA LOS PRODUCTOS Y SERVICIOS. 20](#_Toc2078742)

[9.3. DISEÑO Y DESARROLLO DE LOS PRODUCTOS Y SERVICIOS. 21](#_Toc2078743)

[9.3.1. PLANIFICACIÓN DEL DISEÑO Y DESARROLLO. 21](#_Toc2078744)

[9.3.2. ELEMENTOS DE ENTRADA PARA EL DISEÑO DE DESARROLLO 22](#_Toc2078745)

[9.3.3. CONTROLES DE DISEÑO Y DESARROLLO, 22](#_Toc2078746)

[9.3.4. ELEMENTOS DE SALIDA DEL DISEÑO Y DESARROLLO. 22](#_Toc2078747)

[9.3.5. CAMBIOS EN EL DISEÑO Y DESARROLLO. 22](#_Toc2078748)

[9.4. CONTROL DE LOS PRODUCTOS Y SERVICIOS SUMINISTRADOS EXTERNAMENTE. 22](#_Toc2078749)

[9.4.1. *GENERALIDADES.* 22](#_Toc2078750)

[*9.4.2.* TIPO Y ALCANCE DEL CONTROL DE PROVISIÓN EXTERNA. 22](#_Toc2078751)

[9.4.3. INFORMACIÓN PARA LOS PROVEEDORES. 23](#_Toc2078752)

[9.5. PRODUCCIÓN Y PRESTACIÓN DEL SERVICIO. 23](#_Toc2078753)

[9.5.1. CONTROL DE LA PRODUCCIÓN Y DE LA PROVISIÓN EL SERVICIO 23](#_Toc2078754)

[9.5.2. IDENTIFICACIÓN Y TRAZABILIDAD. 24](#_Toc2078755)

[9.6. PROPIEDAD PERTENECIENTE A LOS CLIENTES O PROVEEDORES EXTERNOS 24](#_Toc2078756)

[9.6.1. PRESERVACIÓN 24](#_Toc2078757)

[9.6.2. ACTIVIDADES POSTERIORES A LA ENTREGA. 24](#_Toc2078758)

[9.6.3. CONTROL DE CAMBIOS. 25](#_Toc2078759)

[9.6.4. LIBERACIÓN DE LOS PRODUCTOS Y SERVICIOS. 25](#_Toc2078760)

[9.6.5. CONTROL DE LOS ELEMENTOS DE SALIDA DEL PROCESO, LOS PRODUCTOS Y SERVICIOS NO CONFORMES. 25](#_Toc2078761)

[10. EVALUACIÓN DEL DESEMPEÑO. 25](#_Toc2078762)

[10.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN. 25](#_Toc2078763)

[10.1.1. SATISFACCIÓN DEL CLIENTE. 26](#_Toc2078764)

[10.1.2. ANÁLISIS Y EVALUACIÓN. 27](#_Toc2078765)

[10.2. AUDITORÍA INTERNA. 27](#_Toc2078766)

[10.3. REVISIÓN POR LA DIRECCIÓN. 27](#_Toc2078767)

[10.3.1. ENTRADAS DE LA REVISIÓN POR LA DIRECCIÓN. 28](#_Toc2078768)

[10.3.2. SALIDAS DE LA REVISIÓN POR LA DIRECCIÓN. 28](#_Toc2078769)

[11. MEJORA. 28](#_Toc2078770)

[11.1. GENERALIDADES 28](#_Toc2078771)

[11.2. NO CONFORMIDAD Y ACCIÓN CORRECTIVA. 28](#_Toc2078772)

[11.3. MEJORA CONTINUA. 29](#_Toc2078773)

[12. SEGURIDAD DE LA INFORMACIÓN 30](#_Toc2078774)

[13. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 30](#_Toc2078775)

[13.1. DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 30](#_Toc2078776)

[13.1.1. CONTROL A.5.1.1. Políticas para la Seguridad de la Información 30](#_Toc2078777)

[13.1.2. CONTROL A.5.1.2 Revisión de las políticas para la Seguridad de la Información 31](#_Toc2078778)

[14. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 31](#_Toc2078779)

[14.1. ORGANIZACIÓN INTERNA 31](#_Toc2078780)

[14.1.1. CONTROL A.6.1.1 Roles y Responsabilidades de la Seguridad de la información. 31](#_Toc2078781)

[14.1.2. CONTROL A.6.1.2 Segregación de tareas. 31](#_Toc2078782)

[14.1.3. CONTROL A.6.1.3 Contacto con Autoridades. 32](#_Toc2078783)

[14.1.4. CONTROL A.6.1.4 Contacto con grupos de especial interés. 32](#_Toc2078784)

[14.1.5. CONTROL A.6.1.5 Seguridad de la Información en la gestión de proyectos. 32](#_Toc2078785)

[14.2. DISPOSITIVOS MÓVILES Y TELETRABAJO 32](#_Toc2078786)

[14.2.1. CONTROL A.6.2.1 Política de dispositivos móviles. 32](#_Toc2078787)

[14.2.2. CONTROL A.6.2.2 Teletrabajo. 32](#_Toc2078788)

[15. SEGURIDAD LIGADA A RECURSOS HUMANOS 32](#_Toc2078789)

[15.1. ANTES DEL EMPLEO 32](#_Toc2078790)

[15.1.1. CONTROL A.7.1.1 Investigación de antecedentes. 32](#_Toc2078791)

[15.1.2. CONTROL A.7.1.2 Términos y Condiciones de Empleo. 33](#_Toc2078792)

[15.2. DURANTE EL EMPLEO 33](#_Toc2078793)

[15.2.1. CONTROL A.7.2.1 Responsabilidades de Gestión. 33](#_Toc2078794)

[15.2.2. CONTROL A.7.2.2 Concienciación, educación y capacitación en Seguridad de la Información. 33](#_Toc2078795)

[15.2.3. CONTROL A.7.2.3 Proceso disciplinario. 34](#_Toc2078796)

[15.3. FINALIZACIÓN O CESE DEL EMPLEO 34](#_Toc2078797)

[15.3.1. CONTROL A.7.3.1 Responsabilidades ante la finalización o cambio. 34](#_Toc2078798)

[16. GESTIÓN DE ACTIVOS 34](#_Toc2078799)

[16.1. RESPONSABILIDAD DE LOS ACTIVOS 34](#_Toc2078800)

[16.1.1. CONTROL A.8.1.1 Inventario de los Activos. 34](#_Toc2078801)

[16.1.2. CONTROL A.8.1.2 Propiedad de los Activos. 34](#_Toc2078802)

[16.1.3. CONTROL A.8.1.3 Uso aceptable de los activos. 34](#_Toc2078803)

[16.1.4. CONTROL A.8.1.4 Devolución de Activos. 35](#_Toc2078804)

[16.2. CLASIFICACIÓN DE LA INFORMACIÓN 35](#_Toc2078805)

[16.2.1. CONTROL A.8.2.1 Clasificación de la información. 35](#_Toc2078806)

[16.2.2. CONTROL A.8.2.2 Etiquetado de la información. 35](#_Toc2078807)

[16.2.3. CONTROL A.8.2.3 Manipulado de la información. 36](#_Toc2078808)

[16.3. MANIPULACIÓN DE LOS SOPORTES 36](#_Toc2078809)

[16.3.1. CONTROL A.8.3.1 Gestión de dispositivos extraíbles. 36](#_Toc2078810)

[16.3.2. CONTROL A.8.3.2 Retirada de soportes físicos. 36](#_Toc2078811)

[16.3.3. CONTROL A.8.3.3 Soportes físicos en tránsito (Transporte de elementos). 37](#_Toc2078812)

[17. CONTROL DE ACCESO 37](#_Toc2078813)

[17.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS 37](#_Toc2078814)

[17.1.1. CONTROL A.9.1.1 Política de Control de acceso. 37](#_Toc2078815)

[17.1.2. CONTROL A.9.1.2 Acceso a redes y servicios en red. 37](#_Toc2078816)

[17.2. GESTION DE ACCESOS DE USUARIOS 37](#_Toc2078817)

[17.2.1. CONTROL A.9.2.1 Registro y baja de usuarios. 38](#_Toc2078818)

[17.2.2. CONTROL A.9.2.2 Provisión de acceso a usuario. 38](#_Toc2078819)

[17.2.3. CONTROL A.9.2.3 Gestión de privilegios de acceso (Administradores). 38](#_Toc2078820)

[17.2.4. CONTROL A.9.2.4 Gestión de autenticaciones de usuarios. 38](#_Toc2078821)

[17.2.5. CONTROL A.9.2.5 Revisión de los derechos de acceso de los usuarios. 38](#_Toc2078822)

[17.2.6. CONTROL A.9.2.6 Retirada o reasignación de los derechos de acceso de los usuarios. 38](#_Toc2078823)

[17.3. RESPONSABILIDADES DE LOS USUARIOS 38](#_Toc2078824)

[17.3.1. CONTROL A.9.3.1 Uso de contraseñas por parte de los usuarios 38](#_Toc2078825)

[17.4. CONTROL DE ACCESOS A APLICACIONES Y SISTEMAS 39](#_Toc2078826)

[17.4.1. CONTROL A.9.4.1 Restricción del acceso a la información. 39](#_Toc2078827)

[17.4.2. CONTROL A.9.4.2 Procedimiento seguros de inicio de sesión. 39](#_Toc2078828)

[17.4.3. CONTROL A.9.4.3 Sistema de gestión de contraseñas. 39](#_Toc2078829)

[17.4.4. CONTROL A.9.4.4 Uso de utilidades con privilegios del sistema. 39](#_Toc2078830)

[17.4.5. CONTROL A.9.4.5 Control de acceso al código fuente de aplicaciones. 39](#_Toc2078831)

[18. CRIPTOGRAFÍA 40](#_Toc2078832)

[18.1. CONTROLES CRIPTOGRÁFICOS 40](#_Toc2078833)

[18.1.1. CONTROL A.10.1.1 Política de uso de controles criptográficos. 40](#_Toc2078834)

[18.1.2. CONTROL A.10.1.2 Gestión de claves para el uso de controles criptográficos 40](#_Toc2078835)

[19. SEGURIDAD FÍSICA Y AMBIENTAL 40](#_Toc2078836)

[19.1. ÁREAS SEGURAS 40](#_Toc2078837)

[19.1.1. CONTROL A.11.1.1 Perímetro de seguridad física. 40](#_Toc2078838)

[19.1.2. CONTROL A.11.1.2 Controles físicos de entrada. 40](#_Toc2078839)

[19.1.3. CONTROL A.11.1.3 Seguridad en oficinas, despachos e instalaciones. 40](#_Toc2078840)

[19.1.4. CONTROL A.11.1.4 Protecciones frente a amenazas externas y ambientales. 41](#_Toc2078841)

[19.1.5. CONTROL A.11.1.5 Trabajo en Áreas seguras (bunker). 41](#_Toc2078842)

[19.1.6. CONTROL A.11.1.6 Áreas de acceso público (recepción, carga y descarga) 41](#_Toc2078843)

[19.2. SEGURIDAD DE LOS EQUIPOS 41](#_Toc2078844)

[19.2.1. CONTROL A.11.2.1 Emplazamiento y protección de equipos 41](#_Toc2078845)

[19.2.2. CONTROL A.11.2.2 Instalaciones de suministro. 41](#_Toc2078846)

[19.2.3. CONTROL A.11.2.3 Seguridad del cableado 42](#_Toc2078847)

[19.2.4. CONTROL A.11.2.4 Mantenimiento de equipos 42](#_Toc2078848)

[19.2.5. CONTROL A.11.2.5 Retirada de materiales propiedad de la empresa. 42](#_Toc2078849)

[19.2.6. CONTROL A.11.2.6 Seguridad de los equipos fuera de las instalaciones. 42](#_Toc2078850)

[19.2.7. CONTROL A.11.2.7 Reutilización o retirada segura de equipos. 42](#_Toc2078851)

[19.2.8. CONTROL A.11.2.8 Equipos de usuario desatendidos. 42](#_Toc2078852)

[19.2.9. CONTROL A.11.2.9 Política de pantalla y escritorios limpios. 42](#_Toc2078853)

[20. SEGURIDAD EN LAS OPERACIONES 42](#_Toc2078854)

[20.1. PROCEDIMIENTOS Y RESPONSABILIDADES DE LAS OPERACIONES 43](#_Toc2078855)

[20.1.1. CONTROL A.12.1.1 Documentación de los procedimientos de Operación. 43](#_Toc2078856)

[20.1.2. CONTROL A.12.1.2 Gestión de Cambios. 43](#_Toc2078857)

[20.1.3. CONTROL A.12.1.3 Gestión de la Capacidad. 43](#_Toc2078858)

[20.1.4. CONTROL A.12.1.4 Segregación de los entornos de desarrollo, prueba y producción. 43](#_Toc2078859)

[20.2. PROTECCIÓN CONTRA CÓDIGO MALICIOSO (MALWARE) 43](#_Toc2078860)

[20.2.1. CONTROL A.12.2.1 Controles contra código malicioso. 43](#_Toc2078861)

[20.2.1.1. DEFINICIONES 43](#_Toc2078862)

[20.2.1.2. OBJETIVO 44](#_Toc2078863)

[20.2.1.3. PROCEDIMIENTO DE INFORME DE INCIDENCIAS POR SOFTWARE MALICIOSO 44](#_Toc2078864)

[20.2.1.4. REGISTROS 44](#_Toc2078865)

[20.3. COPIAS DE SEGURIDAD 44](#_Toc2078866)

[20.3.1. CONTROL A.12.3.1 Copias de seguridad de la información. 44](#_Toc2078867)

[20.4. REGISTRO DE EVENTOS Y MONITORIZACIÓN 44](#_Toc2078868)

[20.4.1. CONTROL A.12.4.1 Registro de eventos. 44](#_Toc2078869)

[20.4.2. CONTROL A.12.4.2 Protección de la información de registro. 45](#_Toc2078870)

[20.4.3. CONTROL A.12.4.3 Registros de Administración y Operación. 45](#_Toc2078871)

[20.4.4. CONTROL A.12.4.4 Sincronización del reloj. 45](#_Toc2078872)

[20.5. CONTROL DE SOFTWARE EN EXPLOTACIÓN 45](#_Toc2078873)

[20.5.1. CONTROL A.12.5.1 Instalación de software en sistemas de operación. 45](#_Toc2078874)

[20.5.2. GESTIÓN DE LA VULNERABILIDAD TÉCNICA 45](#_Toc2078875)

[20.5.3. CONTROL A.12.6.1 Gestión de vulnerabilidades técnicas. 45](#_Toc2078876)

[20.5.4. CONTROL A.12.6.2 Restricciones a la instalación de software. 45](#_Toc2078877)

[20.6. CONSIDERACIONES A LAS AUDITORÍAS DE SISTEMAS DE INFORMACIÓN 45](#_Toc2078878)

[20.6.1. CONTROL A.12.7.1 Controles de auditoría de Sistemas de la Información. 45](#_Toc2078879)

[21. SEGURIDAD EN LAS COMUNICACIONES 45](#_Toc2078880)

[21.1.1. GESTIÓN DE LA SEGURIDAD DE LA RED 45](#_Toc2078881)

[21.1.2. CONTROL A.13.1.1 Controles de red. 45](#_Toc2078882)

[21.1.3. CONTROL A.13.1.2 Seguridad de los servicios de red. 46](#_Toc2078883)

[21.1.4. CONTROL A.13.1.3 Segregación de redes. 46](#_Toc2078884)

[21.2. INTERCAMBIO DE INFORMACIÓN 46](#_Toc2078885)

[21.2.1. CONTROL A.13.2.1 Políticas y procedimientos de transferencia de información. 46](#_Toc2078886)

[21.2.2. CONTROL A.13.2.2 Acuerdos de intercambio de información. 46](#_Toc2078887)

[21.2.3. CONTROL A.13.2.3 Mensajería electrónica 47](#_Toc2078888)

[21.2.4. CONTROL A.13.2.4 Acuerdos de confidencialidad o no divulgación. 47](#_Toc2078889)

[22. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE LA INFORMACIÓN 47](#_Toc2078890)

[22.1. REQUISITOS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN 47](#_Toc2078891)

[22.1.1. CONTROL A.14.1.1 Análisis y especificación de requisitos de seguridad de la información. 47](#_Toc2078892)

[22.1.2. CONTROL A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas 47](#_Toc2078893)

[22.1.3. CONTROL A.14.1.3 Protección de las transacciones de servicios de aplicaciones. 47](#_Toc2078894)

[22.2. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTCONTROL A.14.2.1 Política para el desarrollo seguro. 48](#_Toc2078895)

[22.2.1. CONTROL A.14.2.2 Procedimientos para el control de cambios en los sistemas. 48](#_Toc2078896)

[22.2.2. CONTROL A.14.2.3 Revisión técnica de aplicaciones tras cambios en la plataforma de operación. 48](#_Toc2078897)

[22.2.3. CONTROL A.14.2.4 Restricciones para los cambios de paquetes de software. 48](#_Toc2078898)

[22.2.4. CONTROL A.14.2.5 Principios para sistemas de ingeniería seguros. 48](#_Toc2078899)

[22.2.5. CONTROL A.14.2.6 Entorno seguro de desarrollo. 48](#_Toc2078900)

[22.2.6. CONTROL A.14.2.7 Externalización del desarrollo. 48](#_Toc2078901)

[22.2.7. CONTROL A.14.2.8 Pruebas de seguridad del sistema. 49](#_Toc2078902)

[22.2.8. CONTROL A.14.2.9 Pruebas de aceptación del sistema. 49](#_Toc2078903)

[22.3. DATOS DE PRUEBA 49](#_Toc2078904)

[22.3.1. CONTROL A.14.3.1 Protección de los datos de prueba. 49](#_Toc2078905)

[23. RELACIÓN CON PROVEEDORES 49](#_Toc2078906)

[23.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES 49](#_Toc2078907)

[23.1.1. CONTROL A.15.1.1 Política de seguridad de la información en la relaciones con los proveedores. 49](#_Toc2078908)

[23.1.2. CONTROL A.15.1.2 Requisitos de seguridad en contratos con terceros. 49](#_Toc2078909)

[23.1.3. CONTROL A.15.1.3 Cadena de suministro de Tecnología de la Información y de las Comunicaciones. 49](#_Toc2078910)

[23.2. GESTIÓN DE LA ENTREGA DE SERVICIOS DE PROVEEDORES 49](#_Toc2078911)

[23.2.1. CONTROL A.15.2.1 Control y revisión de la provisión de servicios del proveedor. 49](#_Toc2078912)

[23.2.2. CONTROL A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor. 49](#_Toc2078913)

[24. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 49](#_Toc2078914)

[24.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS 49](#_Toc2078915)

[24.1.1. CONTROL A.16.1.1 Procedimientos y responsabilidades. 49](#_Toc2078916)

[24.1.2. CONTROL A.16.1.2 Notificación de eventos de seguridad de la información. 50](#_Toc2078917)

[24.1.3. CONTROL A.16.1.3 Notificación de puntos débiles de la seguridad. 50](#_Toc2078918)

[24.1.4. CONTROL A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información. 50](#_Toc2078919)

[24.1.5. CONTROL A.16.1.5 Respuesta ante incidentes de seguridad de la información. 50](#_Toc2078920)

[24.1.6. CONTROL A.16.1.6 Lecciones aprendidas del análisis de incidentes de seguridad. 50](#_Toc2078921)

[24.1.7. CONTROL A.16.1.7 Recopilación de evidencias. 50](#_Toc2078922)

[25. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO 50](#_Toc2078923)

[25.1. CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN 50](#_Toc2078924)

[25.1.1. CONTROL A.17.1.1 Planificación de la continuidad de la seguridad de la información. 50](#_Toc2078925)

[25.1.2. CONTROL A.17.1.2 Implantación de la continuidad de la seguridad de la información. 50](#_Toc2078926)

[25.1.3. CONTROL A.17.1.3 Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información. 51](#_Toc2078927)

[26. CUMPLIMIENTO 51](#_Toc2078928)

[26.1. CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES 51](#_Toc2078929)

[26.1.1. CONTROL A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales. 51](#_Toc2078930)

[26.1.2. CONTROL A.18.1.2 Derechos de propiedad intelectual (DPI). 51](#_Toc2078931)

[26.1.3. CONTROL A.18.1.3 Protección de los registros de la organización. 51](#_Toc2078932)

[26.1.4. CONTROL A.18.1.4 Protección y privacidad de la información de carácter personal. 51](#_Toc2078933)

[26.1.5. CONTROL A.18.1.5 Regulación de controles criptográficos. 52](#_Toc2078934)

[26.2. REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN 52](#_Toc2078935)

[26.2.1. CONTROL A.18.2.1 Revisión independiente de la Seguridad de la Información. 52](#_Toc2078936)

[26.2.2. CONTROL A.18.2.2 Cumplimiento de las políticas y normas de seguridad. 52](#_Toc2078937)

[26.2.3. CONTROL A.18.2.3 Comprobación del cumplimiento técnico. 52](#_Toc2078938)

# INTRODUCCIÓN:

# PRESENTACIÓN:

##### Presentación de SOTEC CONSULTING

**SOTEC CONSULTING**, con un equipo de profesionales multidisciplinar de elevada cualificación y amplia experiencia, ofrece servicios de ***consultoría, desarrollo, implantación, integración y mantenimiento de proyectos de tecnologías de la información, negocio y procesos, a través de las diferentes áreas de asistencia técnica, servicios gestionados, diseño y desarrollo de proyectos software y formación****.*

**SOTEC CONSULTING** is composed of a professional, highly prepared and multidisciplinary team. It provides **consultant services, development, implementation, integration, maintenance of IT and business projects, through different technical assistance areas, managed services, design and development systems of software and training projects.**

**SOTEC CONSULTING**, com uma equipe multidisciplinar de profissionais altamente qualificados e com vasta experiência, oferece projetos de **serviços de consultoria, desenvolvimento, implementação, integração e manutenção de tecnologia da informação, negócios e processos em diferentes áreas de assistência técnica, serviços gerenciados, concepção e desenvolvimento de software e formação.**

**SOTEC CONSULTING** es una empresa de origen español fundada en 1996 con una continua proyección internacional que aporta a sus clientes las mejores soluciones para su negocio dentro del ámbito de las Tecnologías de la Información y de las Comunicaciones.

Somos una compañía que colabora con las empresas, nacionales e internaciones, más relevantes de su sector, aportándoles la experiencia y el conocimiento de nuestros consultores con el fin de conseguir la solución más rápida y precisa para sus negocios, asumiendo sus problemas como los nuestros propios.

Gracias a este compromiso nos alineamos totalmente con nuestros clientes para avanzar juntos en el camino hacia el éxito. Un camino donde procuramos cuidar el detalle y hacer posibles sus retos empresariales, asegurándoles una mejor calidad y un progreso continúo en la organización.

Conseguimos alinearnos con cada parte interesada gracias a la capacidad de nuestros profesionales, quienes cuentan con más de 20 años de experiencia en el reclutamiento y selección de perfiles técnicos en el sector IT, tanto del Área de Desarrollo como en el Área de Sistemas.

Además, nuestra sede en Madrid nos permite tener unos costes estructurales equilibrados y proporcionados para ofrecer unas soluciones más rápidas y eficaces.

Porque en **SOTEC CONSULTING** estamos convencidos de que haciendo las cosas correctamente conseguiremos nuestros objetivos y los de nuestros clientes.

# CONTROL DE REVISIONES DEL MANUAL DE CALIDAD

# Preparación, actualización y distribución.

#### Preparación:

Las hojas del Manual se paginarán consecutivamente.

#### Firmas:

Se firmará solamente en la hoja de portada que será la primera del Manual.

#### Actualización:

Se realizará una nueva edición del Manual de Calidad, cuando se produzcan cambios, modificaciones o nuevas versiones en la normativa aplicable.

#### Distribución:

La alta dirección, delega en el Responsable del sistema de Gestión de la Calidad, la responsabilidad de archivar las versiones actualizadas y en curso y distribuirlo a través de la red interna eManage

Control de copias.

# Copias Controladas:

El Responsable del sistema de Gestión de la Calidad de **SOTEC CONSULTING**, con la aprobación de la alta dirección, realizará una copia controlada del Manual de Calidad para la consulta del mismo por parte de todo el personal de la empresa.

#### Copias no Controladas:

Serán las copias del Manual que se entreguen a aquellas personas o entidades a las cuales no se van a enviar las revisiones que se vayan produciendo en el mismo.

Realizamos también un **Control A.12.3.1.** de copias de seguridad de la información, que se encuentra en el PSI-30 Procedimiento de Back up que se ubica en eManage; y un **Control A.12.3.1**. Copias de seguridad de la información, localizado en el PSI 03 Procedimiento de backup.

Estas copias no controladas, son las que se publican en la página web, o las que se le entrega a los empleados cuando se incorporan en la empresa.

# POLÍTICA DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

# Declaración de la política de Calidad y Seguridad de la Información.

En **SOTEC**, tenemos el objetivo de alcanzar una posición de liderazgo en el ámbito de la **consultoría, desarrollo, implantación, integración y mantenimiento de proyectos de tecnologías de la información, negocios y procesos, a través de las diferentes áreas de asistencia técnica, servicios gestionados, diseño y desarrollo de proyectos software y formación.**

#### Así mismo, reconoce la importancia de identificar y proteger sus activos de información, conforme a la norma de referencia evitando la destrucción, divulgación, modificación y la utilización no autorizada de toda información relacionada con las partes interesadas, previos, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia gestión y otros conceptos. De esta manera se compromete también a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.

Nuestra política es brindar los máximos niveles de calidad a los servicios e incorporar a los mismos, la capacidad y la suficiencia de respuesta, la habilidad y la competencia técnica mediante la incorporación de activos de primera línea constituyéndonos como una organización que incorpora los valores de una empresa seria que gestiona sus recursos con eficacia y eficiencia.

La actividad de Sotec Consulting al completo**,** está orientada a satisfacer plenamente las necesidades de nuestros clientes y resto de partes interesadas, para lo que precisamos contar con la plena implicación de empleados y colaboradores. Asimismo aseguramos la información como activo fundamental de la organización.

La Política de Calidad y Seguridad de la Información y el Código Ético y de Conducta constituyen los pilares básicos dentro de la Política General de la empresa estableciendo y minimizando, de esta manera los riesgos a los que se expone la información, estableciendo y revisando los objetivos de calidad y seguridad para obtener la plena satisfacción de las partes interesadas..

Por esta razón, y con el fin de alcanzar los objetivos marcados, la Dirección adopta el compromiso de dedicar a esta tarea todo su potencial económico, tecnológico y humano de forma que la organización de la empresa, su política de inversiones, el desarrollo de nuevos métodos y los recursos humanos y materiales, estén orientados prioritariamente a satisfacer las necesidades en esta materia, de las partes interesadas y sujetos a las directrices establecidas por la Dirección.

Nuestros principios de actuación son:

* + - * **Lograr la satisfacción plena de nuestros clientes,** estudiando todos los servicios desde diferentes perspectivas optimizando su funcionalidad.
      * **Creación y mantenimiento de una cultura de Calidad y Seguridad**, que sea asumida por la totalidad de los empleados y colaboradores y que constituya la base de nuestra actividad.
      * **Dirigir nuestros esfuerzos a una mejora continua** de la calidad de nuestros servicios y mejora en la eficacia de nuestros procesos, de tal forma que la **capacidad de reacción** y **adaptabilidad** supere las expectativas de mercado.
      * Cumplir todos los requisitos de las Normativas y Legislación aplicables y servir de referencia a terceros para establecer los Objetivos de Calidad.
      * Garantizar a los empleados el nivel de formación, motivación y los medios técnicos necesarios para el eficiente desarrollo de sus actividades.
      * Asegurar la confidencialidad, entendida como la garantía del acceso a la información únicamente de los usuarios autorizados: establecer controles de acceso.
      * Establecer anualmente objetivos con relación al sistema de gestión de calidad y de la seguridad la información
      * Identificar riesgos de procesos internos y aquellos que sean operados con terceros. Desarrollar un proceso de análisis del riesgo identificado.
      * Asegurar la integridad de los activos, para garantizar la preservación de la información de forma completa y exacta: utilizar apropiadamente los activos y realizar copias de seguridad.
      * Asegurar la disponibilidad, de manera que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran. La seguridad de la información se consigue implantando un conjunto adecuado tanto de controles, como de políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles han sido establecidos para asegurar que se cumplen los objetivos específicos de seguridad de la empresa.
      * Innovación: Fortalecer los medios de innovación en procesos y tecnología, permitiendo cumplir con mayor calidad las necesidades de nuestras partes interesadas, de modo que seamos más eficaces y productivos.
      * Sancionar cualquier violación a esta política o cualquier código o procedimientos de la empresa.
      * Los departamentos de calidad y de operaciones son responsables directos del mantenimiento de esta política, de brindar consejo y guía para su implementación, e investigar toda violación reportada por el personal.

Se velará por el Cumplimiento de los requisitos legales y normativos, sirviendo éstos como marco de referencia para establecer los objetivos de calidad en el desarrollo de nuestra actividad. .

Esta política adecuada a nuestra organización es comunicada al personal y colaboradores y entendida por el mismo, existiendo un compromiso por su parte de implicación y compromiso con la Gestión de la Calidad.

Los empleados y colaboradores de **SOTEC CONSULTING** son informados acerca de las políticas internas de la Compañía, a través de la entrega de la política en el momento de incorporarse en su puesto de trabajo, y con el acceso permanente al documento en eManage.

# OBJETO Y CAMPO DE APLICACIÓN.

El presente manual, constituye la información documentada en la que **SOTEC CONSULTING** basa su Sistema de gestión de la Calidad y Seguridad de la Información.

La elaboración del Manual, así como sus sucesivas revisiones pretenden adecuar continuamente la gestión de los procesos llevados a cabo en **SOTEC CONSULTING**, adaptándolo a las necesidades de cada momento.

Los procesos, constituyen el conjunto de información documentada donde se describen de forma detallada los trabajos, actividades u operaciones a realizar en **SOTEC CONSULTING.** Engloban los procedimientos que se siguen en la empresa para desarrollar nuestra actividad.

El objeto del presente manual, es establecer las directrices generales y el alcance del Sistema de gestión de la calidad y de seguridad de la información de **SOTEC CONSULTING**.

**SOTEC CONSULTING** se compromete a que todo su personal conozca y cumpla lo establecido en este manual y en todo el sistema de calidad en general.

El presente manual sigue el procedimiento establecido, y cubre los requisitos del Sistema de gestión de calidad que establece la Norma Técnica UNE-EN-ISO 9001 de Gestión de Calidad, y UNE-EN ISO/IEC 27001.

# REFERENCIAS NORMATIVAS.

A efectos de este Manual de Calidad, **SOTEC CONSULTING** toma como referencia las siguientes normas:

-UNE-EN ISO 9001: 2015, Sistemas de gestión de la calidad. Requisitos.

-UNE-EN ISO 9000: 2015, Sistemas de gestión de la calidad. Fundamentos y vocabulario.

* UNE-EN ISO/IEC 27001:2017, Sistemas de gestión de la Seguridad de la Información Requisitos.

# TÉRMINOS Y DEFINICIONES.

##### Términos:

* + SGC: Sistema de gestión de la Calidad.
  + SGSI: Sistema de gestión de la Seguridad de la Información
  + SOTEC: SOTEC CONSULTING.
  + RRHH: Recursos Humanos.
  + EManage: Es la aplicación interna de Sotec Consulting mediante la cual el staff de la compañía desempeña su trabajo diario en la empresa. Está dotada de diferentes pestañas, en base a las necesidades de cada departamento, por lo que también está en constante mejora.

El acceso a ella está supeditado al rol de cada empleado, y de esto dependerá la habilitación de permisos para utilizar unas herramientas u otras. Garantiza que los accesos se hagan con total seguridad, ya que está protegido mediante usuario y contraseña diferentes para cada empleado que cambian cada cierto periodo de tiempo.

##### Definiciones:

* + Alta dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel.
  + Acción correctiva: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.
  + Auditoría interna: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.
  + Calidad: Grado en el que un conjunto de características inherentes cumple con los requisitos.
  + Conformidad: Cumplimiento de un requisito.
  + Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.
  + Mejora: Actividad recurrente para mejorar el desempeño.
  + Parte interesada: persona u organización que podría recibir o que recibe un producto o un servicio destinado a esa persona u organización o requerido por ella.
  + Procedimiento: forma especificada para llevar a cabo una actividad o un proceso.
  + Proceso: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.
  + Producto o servicio: Resultado de un proceso o un conjunto de procesos.
  + Requisito: Necesidad o expectativa establecida, generalmente implícita u obligatoria.
  + Satisfacción del cliente: Percepción del cliente sobre el grado en que se han cumplido sus requisitos y expectativas.

# CONTEXTO DE LA ORGANIZACIÓN.

# CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO.

**SOTEC CONSULTING** a través de la dirección, establece la estrategia de la compañía, determina, controla y revisa los aspectos externos e internos que son relevantes para su propósito y que afectan a su capacidad para el logro de los resultados deseados.

**-Aspectos Internos.-**Se definen como aquellas cuestiones relacionadas con los valores y cultura organizacional, capacitación y desarrollo:

#### Certificación ISO 9001 e ISO 27001. Valores y cultura organizacionales

Creación y mantenimiento de una cultura de Calidad y Seguridad de la Información, que sea asumida por la totalidad de los empleados y que constituya la base de nuestra actividad, y que nos permita obtener las certificaciones ISO 9001 y 27001 correspondientes.

Nuestra **misión** es ser socio tecnológico de nuestros clientes y parteners, cuidando el más mínimo detalle para impulsar su negocio, trabajando siempre bajo un mismo lema: DOING THE RIGHT THING.

**Visión**. En Sotec somos una compañía de ámbito internacional que apuesta por las personas, la innovación y el compromiso para dar a nuestros clientes el mejor valor añadido en la prestación de nuestros servicios.

Nuestros **valores** son determinación, creatividad, integridad, cuidado al detalle, hands on, innovación, respeto, compromiso, motivación, proactividad, trabajo en equipo, honestidad, valor añadido, honestidad, actitud, constancia, equilibrio, ilusión, responsabilidad, confidencialidad, perseverancia, y development on the go.

#### Procesos de la organización:

Ejercemos nuestra actividad en base a procesos desarrollados en nuestra plataforma eManage, que permiten una mejor planificación y estructuración del trabajo. Es un modelo diseñado para tener un seguimiento y una mejora continua de la empresa, independientemente del cambio de circunstancias de la misma.

Contamos con una pestaña en eManage que recoge todas las áreas y todos los departamentos, asignándole a cada uno, sus respectivos procesos, en forma de actividad. Cuando se accede a planificación, en forma de agenda distribuida por horas. A continuación, se abre una nueva actividad en base al trabajo que vayamos a realizar. Esta actividad tiene asignados unos determinados documentos, necesarios para dicha actividad y que describen cómo desarrollar la tarea.

En el caso de que aparezca la necesidad de nuevos procesos, existe la opción de crear nuevas actividades, o incluir nuevos procedimientos a través de la asignación de documentos a las actividades.

Existe un listado con todos los procedimientos de la compañía en eManage, en el apartado de Gestor documental, en la opción “exportar datos a Excel”.

#### Áreas:

Sotec Consulting, está divido en varias áreas en la que se encuentran profesionales especializados, desarrollando su actividad. Cada área tiene un líder que organiza la actividad de cada uno de los empleados que forman parte de su equipo.

La empresa se divide en:

* + - * Comercial
      * Operaciones
      * Recursos Humanos
      * Marketing
      * Administración y Servicios Generales
      * Dirección
      * Staffing

-

#### Capacitación y desarrollo:

Garantizar a los empleados el nivel de formación, motivación y los medios técnicos necesarios para el eficiente desarrollo de sus actividades.

Tenemos implantada una capacitación inicial, a través de la cual, las nuevas incorporaciones adquieren un conocimiento general, tanto de la estructura de la compañía como de su funcionamiento. Está capacitación incluye tanto documentación de bienvenida con las normas que rigen en la empresa, como los procedimientos específicos asignados a su puesto y conforme van desarrollando su labor en la compañía también tienen acceso al legado que dejan todos los miembros de la compañía. Esta capacitación está ubicada en eManage cuando accedemos al apartado de Planificación y Nueva actividad.

Contamos también con un plan de formación interna, a través del cual gestionamos cursos con tripartita. Exponemos un catálogo de cursos que podemos ofertar a todos los empleados de la compañía, para facilitarles su desarrollo profesional a través de esta formación. En el caso de que no exista la posibilidad de tripartita, se podrán estudiar otras opciones, valorando el grado de necesidad de formación.

Tenemos la opción en nuestra plataforma de gestión de eventos. Existe una funcionalidad, a través de la cual, se puede dejar el denominado “legado” de todo lo adquirido en esos eventos a los que asistimos. De esta manera mantenemos la información para los empleados, y futuras incorporaciones.

**-Aspectos Externos.** Se definen como aquellas cuestiones derivadas de los entornos jurídico, tecnológico y social, tales como:

#### Jurídico:

Cumplir todos los requisitos de las Normativas y Legislación aplicables y servir como marco de referencia para establecer los Objetivos de Calidad.

Asegurar la confidencialidad, entendida como la garantía del acceso a la información únicamente de los usuarios autorizados: establecer controles de acceso.

Asegurar la integridad de los activos, entendida como la preservación de la información de forma completa y exacta: utilizar apropiadamente los activos y realizar copias de seguridad.

#### Tecnológico:

Dirigir nuestros esfuerzos a una mejora de la calidad de nuestros servicios y mejora en la eficacia de nuestros procesos, de tal forma que la capacidad de reacción y adaptabilidad supere las expectativas de mercado.

Asegurar la disponibilidad, entendida como acceso a la información en el instante en el que el usuario la necesita.

#### Social:

Lograr la satisfacción plena de la parte interesada, estudiando todos los servicios desde diferentes perspectivas optimizando su funcionalidad.

# COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS.

SOTEC CONSULTING investiga, identifica, revisa, controla y hace seguimiento de las partes interesadas en sus procesos operativos, procedimientos e instrucciones de trabajo. A efecto de suministrar los servicios que satisfagan a la parte interesada y cumplir con los requisitos legales. La información relativa a las partes interesadas de la compañía podrá encontrarse en el Informe de Contexto de la Organización, documento en el que se recogen las necesidades y expectativas de las partes interesadas clasificando las mismas en externas e internas.

SOTEC CONSULTING presta especial atención a los empleados y colaboradores ya que son el motor de la compañía constituyendo la parte interesada interna de la misma.

## Como partes interesadas externas destacamos las alianzas, los clientes, los proveedores, las Administraciones Públicas, las Universidades y centros formativos, la competencia y los candidatos, que cuentan con la característica de que podrán pasar a constituir una parte interesada interna de Sotec en cualquier momento.

# DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

## El presente manual, constituye la información documentada en la que SOTEC CONSULTING basa su Sistema de Calidad y Seguridad de la Información, y constituye la guía de referencia básica, para las operaciones que afectan a nuestros servicios.

## Su alcance abarca los servicios de consultoría, desarrollo, implantación, integración y mantenimiento de proyectos de tecnologías de la información, negocio y procesos, a través de las diferentes áreas de asistencia técnica, servicios gestionados, diseño y desarrollo de proyectos software y formación.

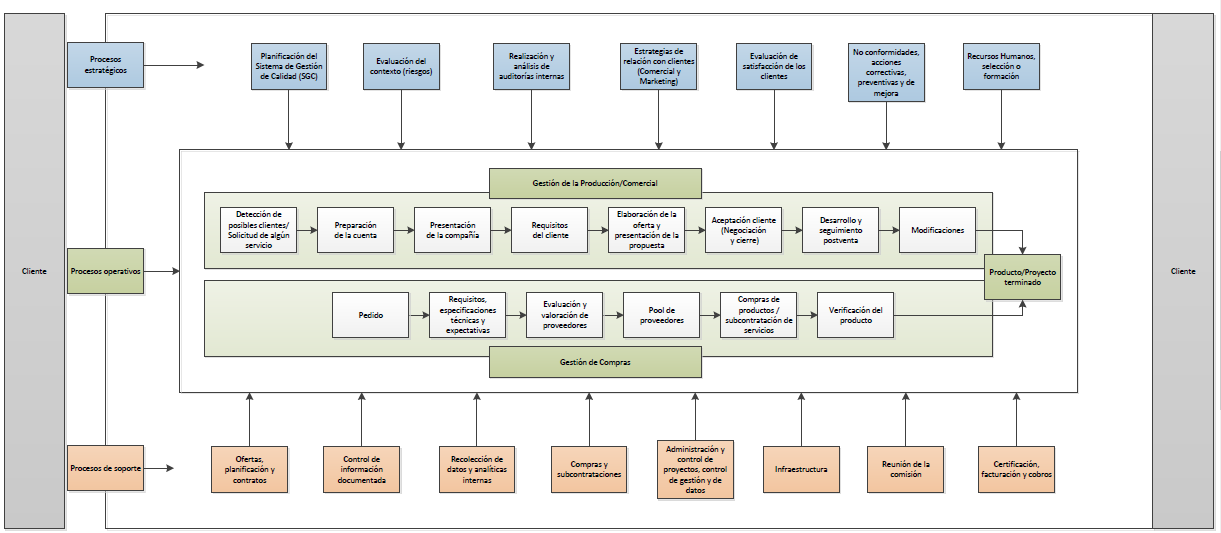
## La elaboración del Manual, así como sus sucesivas revisiones pretenden adecuar continuamente la gestión de los procesos llevados a cabo en Sotec consulting, adaptándolo a las necesidades de cada momento.

# SISTEMA DE GESTIÓN DE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN Y SUS PROCESOS

**SOTEC CONSULTING** ha establecido, implantado y mantiene un Sistema de Gestión de la Calidad y Seguridad de la Información de acuerdo a lo establecido en la **Norma UNE-EN- ISO 9001 y UNE-EN ISO/IEC 27001**, y ha implantado la herramienta eManage para el seguimiento, medición y análisis de los procesos a través de indicadores y ha establecido un compromiso para lograr los resultados planificados y alcanzar la mejora según los datos obtenidos.

Este Sistema de Gestión de la Calidad y Seguridad es de obligado cumplimiento interno y se ha diseñado e implantado para garantizar la conformidad de los servicios con los requisitos establecidos.

Para ello, existen unos procesos implantados en Sotec, localizados en nuestra plataforma eManage. Cada proceso se divide en una serie de actividades, que a su vez, llevan asignados unos documentos donde se explica el procedimiento a seguir para realizar esa actividad.



# LIDERAZGO.

# LIDERAZGO Y COMPROMISO.

# LIDERAZGO Y COMPROMISO PARA EL SISTEMA DE GESTIÓN DE CALIDAD.

La Dirección de **SOTEC CONSULTING** es consciente del papel motor que desempeña el compromiso de la dirección en la implantación y desarrollo del Sistema de Gestión de la Calidad, así como de la mejora de su eficacia. Por ello promueve y desarrolla un Sistema de gestión que garantice la calidad y la seguridad de la información, con apoyo de las normativas UNE-EN ISO correspondientes.

Expresa su compromiso a través de la Política definida y diseñada en atención a los propósitos de Calidad, y a la viabilidad de los mismos dentro de la empresa.

Se compromete a:

* + - * Definir, documentar e implementar un Sistema de Gestión de la Calidad y Seguridad de la información, a través de la Política y mejorar su eficacia.
      * Difundir este sistema y esta política para que sean conocidos, implantados y mantenidos al día por toda su organización.
      * Establecer y documentar los objetivos de la calidad.
      * Poner los medios necesarios para que este Sistema y esta Política sean adecuados a los objetivos de Sotec consulting**,** y a las expectativas y a las necesidades de sus partes interesadas, incluyendo los requisitos tanto legales como reglamentarios.
      * Identificar las necesidades de recursos para cumplir nuestro Sistema de Gestión y la Política y proporcionar estos recursos cuando sean necesarios.
      * Realizar periódicamente revisiones de nuestro Sistema de Gestión de la Calidad. Anualmente en el mes de Noviembre mediante auditorías internas.

# ENFOQUE AL CLIENTE.

**SOTEC CONSULTING,** orienta su Sistema de Calidad hacia la satisfacción de la parte interesada, determinando de forma inequívoca los requisitos de éste antes de realizar los trabajos.

Asegura que se satisfacen las necesidades y expectativas de las partes interesadas actuales y potenciales, e intenta mejorar su nivel de satisfacción teniendo en cuenta las siguientes necesidades:

* + - * Determinar los requisitos de la parte interesada.
      * Comunicación periódica con la parte interesada para facilitarle información sobre el desarrollo de la operación.
      * Cumplimiento de los plazos contractuales.
      * Realizar una prospección del nivel de satisfacción de la parte interesada, analizar los resultados obtenidos y aplicar las mejoras pertinentes.

Para cumplir con esas necesidades, se sigue un procedimiento con sus respectivas actividades asignadas, como se refleja en nuestro Gestor documental en eManage.

# *POLÍTICA DE CALIDAD.*

Se corresponde con lo indicado en el apartado 1.3 de este Manual de Calidad. Con esta política se asume un compromiso que lleva a un concepto integral de la Calidad, cuyo principio fundamental es que ésta se desarrolla de forma progresiva mediante aportaciones de todas y cada una de las partes y actividades de la empresa. La política será revisada anualmente en la revisión del sistema por la dirección.

-Comunicación de la política

Esta política de Calidad y Seguridad de la Información se encuentra disponible para las partes interesadas, en la página web de SOTEC. Igualmente, ésta se comunica a los empleados recién incorporados, quienes firman un justificante tras haber recibido un documento con la política, declarando que la entienden y que van a proceder a aplicarla. Así mismo, esta política se encuentra al alcance de todos los empleados, en la plataforma de trabajo eManage, donde pueden consultarla en el momento que deseen.

# ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN.

La Dirección de Sotec consulting ha definido la estructura de la empresa de manera que el personal conozca sus responsabilidades, atribuciones e interrelaciones de manera clara y precisa.

Las funciones y responsabilidades, así como las relaciones existentes entre cada uno de los miembros de **SOTEC CONSULTING**, se describen en los perfiles de puesto específicos de los que se dispone para cada puesto de trabajo y que son aprobados por Dirección y definidos de acuerdo a lo descrito en procedimiento de Roles y Funciones de RRHH y recogido en Emanage.

**Organización interna**Sotec consulting tiene reflejada su organización en un Organigrama en eManage. Se encuentra en la herramienta Emanage en la pestaña de Puesto  Organigrama.

Además existe la herramienta de **Mi Perfil**, donde aparece también el organigrama de la compañía, de forma horizontal y en cascada. En esta pestaña también aparece el rol y responsabilidad que se le asigna a cada puesto de la compañía, así como, los procesos que tiene asignados ese puesto con sus respectivos procedimientos. Aparecen reflejados también, tanto los KPIs de cada empleado, como el desempeño continuo de su labor, teniendo como referencia unos parámetros fijos.

# PLANIFICACIÓN.

# ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES.

La empresa gestiona los riesgos y oportunidades en base al análisis estratégico de la compañía. Cada año, se establecen unos **objetivos** con unas acciones asignadas, en base a nuestro posicionamiento en el sector, estudiando el contexto situacional en el que nos encontramos.

Cada departamento realiza un informe DAFO anual, en el que se refleja la situación en la que nos encontramos, los riesgos que pueden aparecer y las nuevas oportunidades a las que aspiramos.

Con los riesgos y oportunidades identificados, se realiza una valoración de los mismos de acuerdo al Procedimiento de Valoración del Riesgo.

La gestión de los riesgos y oportunidades se lleva a cabo por el Responsable de Calidad que tiene un excel de Riesgos y oportunidades donde realiza un seguimiento de los mismos y se hace figurar las conclusiones de la revisión por Dirección de los mismos, además de en el Acta de Revisión. Se asociará a cada uno de ellos una acción y se valorarán teniendo en cuenta dos criterios variables: Impacto y probabilidad.

El análisis de estos dos criterios nos permitirá clasificar los riesgos en tres grupos: riesgos razonablemente aceptables, riesgos intermedios y riesgos significativos.

En base a esto, establecemos unos objetivos, a los que se les hace un seguimiento periódico, mediante reuniones de seguimiento. Por ejemplo: reuniones semanales de Forecast.

#### Planificación del Sistema de Gestión de la Calidad y Seguridad de la Información:

El departamento de Calidad junto con la alta dirección asume la responsabilidad de la planificación de la calidad. Esta planificación se enfocará en la definición de los procesos necesarios para cumplir eficazmente los objetivos de calidad y los requisitos, la conservación de la efectividad y mejora del sistema durante los cambios y después de efectuados los mismos y la aportación de los recursos humanos económicos y materiales necesarios para ello.

Para llevar a cabo esta planificación se tendrán en cuenta los siguientes aspectos:

* + - La planificación estratégica y los objetivos para definir hacia dónde quiere ir la empresa.
    - La planificación de la carga de trabajo, para conseguir la eficiencia operacional del servicio prestado.
    - Las necesidades de las partes interesadas.
    - Los cambios e imprevistos que surjan, para adaptarse de forma eficiente

Esta planificación del Sistema de Gestión de la Calidad se analizará a la vez que la revisión del Sistema por la Dirección. Si bien es cierto, el desarrollo de estas acciones y alcance de objetivos, se podrá analizar en reuniones de seguimiento periódicas por parte de la dirección con los responsables de cada Departamento.

Las acciones que se hayan asignado a los objetivos, se irán ejecutando conforme a los procedimientos establecidos en Sotec Consulting. Estos procedimientos aparecen documentados en la **planificación** de eManage. Cuando se va a realizar una actividad, tiene asignada una documentación que refleja el procedimiento a seguir para llevarla a cabo.

Cuando las circunstancias cambian y es necesario tomar acciones que no se contemplan en nuestros procedimientos, se pueden crear nuevos y asignarlos a la actividad correspondiente en eManage.

# OBJETIVOS DE LA CALIDAD, SEGURIDAD Y PLANIFICACIÓN PARA LOGRARLOS.

El **Responsable del sistema de Gestión de la Calidad** utiliza herramientas que le permitan establecer criterios para la adopción de acciones preventivas, a fin de evitar la aparición de no conformidades, en todas las fases de la prestación de servicio.

El Responsable del sistema de Gestión de la Calidad mantiene los registros de las no Conformidades detectadas y las acciones correctivas y evolutivas establecidas. Realiza un seguimiento periódico del estado de las diferentes acciones que se ejecutan para la mejora continua.

Los objetivos particulares en materia de calidad y seguridad de la información, considerados como metas definidas y cuantificadas, que van a servir de base para la planificación de la realización del servicio, serán fijados anualmente por la Dirección.

Estos objetivos se plantean, con un previo estudio de los objetivos de cada área de la compañía, por parte de su responsable. Posteriormente, son revisados por la alta dirección, y en base a ellos, realiza la planificación de objetivos anual. Este procedimiento se encuentra recogido en eManage.

En el establecimiento de estos objetivos se deberá considerar:

* + - Las necesidades actuales y futuras.
    - Los niveles de satisfacción de las partes interesadas.
    - Los resultados de las auditorías internas y revisiones del sistema por la dirección.
    - Recursos necesarios para cumplir los objetivos.

Los objetivos de calidad y seguridad serán comunicados al personal de Sotec Consulting para que puedan contribuir a su logro. Estos objetivos se definen en el registro “Objetivos” así como el seguimiento realizado a los mismos, dichos objetivos están subidos a Emanage en el gestor documental, en el Grupo Gerentes  ISO 9001 Objetivos e ISO 27001> Objetivos.

# PLANIFICACIÓN DE LOS CAMBIOS.

La gestión de cambios en cuanto a calidad y seguridad de la información se refiere, la planifican los responsables de Calidad y Operaciones, respectivamente. Ellos serán los encargados de establecer una relación periódica y directa con los responsables de cada área, de tal manera, que se puedan detectar las necesidades de cambio de manera rápida y eficaz.

La Dirección de cada área asume la responsabilidad de la planificación de la calidad. Esta planificación se enfocará en la definición de los procesos/procedimientos necesarios para cumplir eficazmente los objetivos de calidad y los objetivos estratégicos de la compañía, la conservación de la efectividad e integridad del sistema durante los cambios y después de efectuados los mismos y la aportación de los recursos humanos económicos y materiales necesarios para ello.

Esta planificación del Sistema de Gestión de la Calidad se realizará a la vez que la revisión del Sistema por la Dirección. Si bien es cierto, el estudio de recursos durante el año se podrá analizar en reuniones periódicas de la dirección con los responsables de cada departamento

# SOPORTE

# RECURSOS

# PERSONAS

Sotec Consulting**,** cuenta con profesionales multidisciplinares de elevada cualificación y amplia experiencia, por lo que son competentes a la hora de cumplir los requisitos que se establecen, en base a la educación, formación, habilidades y/o la experiencia propia señalada anteriormente.

Cada rol en la compañía tiene asignadas unas funciones, y unos requisitos que debe cumplir a nivel formativo y laboral, para poder incorporarse a la empresa. Esta información aparece reflejada en cada puesto del organigrama que está ubicado en eManage en la pestaña de Puesto  Organigrama.

Añadir que cada usuario en eManage, tiene acceso a la herramienta Mi Perfil, en la cual aparece reflejada toda su información dentro de Sotec Consulting. Muestra el rol que desempeña dentro de la empresa, las funciones que ha de desarrollar, sus competencias, los procesos y las respectivas actividades asignadas para su desarrollo, exámenes, KPIs y desempeño en la empresa.

# INFRAESTRUCTURA*.*

La Dirección definirá la infraestructura teniendo en cuenta las necesidades actuales y las futuras expectativas. La infraestructura incluirá recursos tales como el espacio de trabajo, mobiliario, equipos y programas informáticos, etc.

**SOTEC CONSULTING** dispone de unas instalaciones amplias, limpias y ordenadas donde poder desarrollar el trabajo de manera eficaz. Se asegura que los equipos y materiales utilizados para la prestación del servicio durante las distintas etapas del proceso llevado a cabo son los adecuados, contando con un inventariado registrado en la herramienta interna de Sotec, eManage, en el apartado Sistemas/Control dispositivos.

# AMBIENTE PARA LA OPERACIÓN DE LOS PROCESOS.

**SOTEC CONSULTING,** asegura que las condiciones de trabajo (temperatura, amplitud, orden y limpieza) son adecuadas para desarrollar adecuadamente las actividades, asimismo se proporciona y mantiene el ambiente de trabajo necesario para lograr la conformidad con los requisitos del servicio solicitado.

# RECURSOS DE SEGUIMIENTO Y MEDICIÓN.

El seguimiento y medición de los objetivos planificados, se realiza a través de las diferentes reuniones de seguimiento.

* + - * Reuniones de Forecast y Pipeline: son reuniones semanales, para comprobar la evolución de la empresa en el aspecto comercial.
      * Reuniones de seguimiento individuales, para evaluar el desempeño diario, y establecer nuevas acciones. Los responsables transmiten los objetivos establecidos por la dirección, y adaptan las tareas diarias de los empleados a los mismos.
      * Mi Perfil: en la herramienta Mi Perfil se reflejan todos los datos relacionados con el empleado.

Aparece un organigrama tanto en horizontal como en cascada, para que los empleados conozcan la estructura de la organización.

En el apartado de Mi Puesto  Mi perfil, aparecen reflejados todos los datos y estadísticas del trabajo de cada empleado. Se muestran los procesos, actividades y documentación que se le asigna a cada emplead

Están tanto“Mis competencias” y “Pruebas de competencia” como “Mis procesos”, “Mis actividades”, Mis documentos de actividades” que muestran al empleado los procesos que tiene asignados para el desempeño correcto de su labor en la empresa.

Además están incluidos mis procesos, mis actividades, mis documentos de actividades, mis exámenes de actividades, mis KPIs, mi desempeño, mi formación.

# CONOCIMIENTOS DE LA ORGANIZACIÓN.

Sotec Consulting determina los conocimientos necesarios para la operación de los procesos de conformidad, en atención al punto 8.1.2 de este Manual. De igual manera, garantiza el mantenimiento y la accesibilidad del conocimiento mediante el la pestaña formación, ubicada en el gestor documental de eManage y asociado al grupo de RRHH, donde se determina la instrumentalización de los programas de capacitación, que permiten inducir, preparar, actualizar y certificar al personal, para un mejor desempeño de sus funciones.

# COMPETENCIA.

El personal dedicado a las actividades relacionadas con la prestación del servicio y gestión de la calidad y seguridad de la información, tiene la formación y habilidades adecuadas, encontrándose debidamente cualificado, conforme a los requisitos y a las necesidades derivadas de los requerimientos de los objetivos planteados, de los servicios ofertados y de las características de las partes interesadas actuales y potenciales, conforme a los Roles y Funciones determinados en la empresa para los mismos.

# COMPETENCIA, TOMA DE CONCIENCIA Y FORMACIÓN

Se tiene establecido y se mantiene el Procedimiento de Formación, ubicado en el gestor documental de eManage y asociado al grupo de RRHH, para determinar las necesidades de formación. Asimismo, Sotec promueve la participación y el desarrollo:

* + - Capacitación Inicial organizado y gestionado en eManage a través de su planificador
    - Formación continúa

A través de la entrega del Manual de bienvenida y la Política de calidad y seguridad de la información, nos aseguramos de que los empleados tengan conocimiento de nuestro modo de trabajar en la compañía.

# COMUNICACIÓN*.*

La Dirección establece los canales de comunicación interna dentro de la empresa teniendo en cuenta los procesos del Sistema de Gestión de la Calidad y Seguridad de la Información de manera eficaz.

Por el tamaño y características de la organización, generalmente la transmisión de la información entre departamentos es verbal.

#### Difundir la política y objetivos de calidad y seguridad:

La Política de Calidad y Seguridad está a disposición del público y Responsable del sistema de Gestión de la Calidad se encargará de difundirla entre sus empleados, como se encuentra recogido en el apartado 6.2. del presente manual.

Asimismo, el Responsable del sistema de Gestión de la Calidad comunicará los objetivos de calidad a los Responsables de Departamento.

#### Informe de Revisión del Sistema por la Dirección:

Según lo expuesto en el punto 10.3, el Responsable del sistema de Gestión de la Calidad remite una copia del acta de revisión a todos los asistentes a la misma.

El procedimiento de comunicación se encuentra documentado en eManage, en el gestor documental apartado Markenting>Capacitación>Común administración.

# INFORMACIÓN DOCUMENTADA.

El Sistema de Gestión de la Calidad y Seguridad de Sotec queda definido en la siguiente información documentada:

* Manual de Calidad.
* Procesos asignados a actividades en eManage.
* Formatos y Registros eManage.
* Gestor Documental de eManage.

# GENERALIDADES.

El Manual de Calidad y Seguridad de la Información, es la información documentada básica del Sistema de Calidad en el que se establece la política de calidad de la Dirección de Sotec Consulting.

Este Manual de Calidad hace referencia a los procedimientos del Sistema de Gestión de la Calidad, refleja la manera de actuar de la empresa obligando a todos sus miembros a llevar a cabo todas las actividades según lo descrito en él y persigue el cumplimiento de la Norma **UNE-EN-ISO** correspondiente

La redacción y revisión del presente Manual corresponde al Responsable de Gestión de la Calidad debiendo estar aprobado por él mismo y por la alta dirección

La elaboración del Manual, así como sus sucesivas revisiones pretenden adecuar continuamente la gestión de los procesos llevados a cabo en Sotec Consulting aptándolo a las necesidades de cada momento.

# CREACIÓN Y ACTUALIZACIÓN.

#### Control de los Registros:

Contamos con unos manuales sobre control de la información que se basan en:

* + - Gestión del software: donde se establecen los repositorios y las reglas sobre la gestión de la documentación.
    - Manual de clasificación y tratamiento de la información: donde establecemos un criterio de la clasificación de la información, reglas para su correcto manejo y protección y su respectivo control.

Todos los registros de gestión de la calidad ( informes de alta dirección, auditorías internas, objetivos anuales… )se conservan para demostrar la conformidad con los requisitos especificados y el funcionamiento eficaz del Sistema de Gestión de la Calidad.

Estos registros son legibles e identificables, están guardados y conservados adecuadamente para su fácil recuperación y en unas condiciones que eviten su deterioro, daño o pérdida. Se encuentran en eManage en el apartado de gestor documental, en cada carpeta ISO correspondiente.

Tenemos establecido y registramos el tiempo mínimo de conservación de los registros de calidad. Salvo que esté establecido contractualmente, los registros de calidad estarán a disposición de las partes interesadas durante un periodo mínimo de 3 años, a excepción de otros que por requisito legal sea superior.

##### Actualización:

Cualquier modificación ya sea en una sola hoja o en varias exigirá un control de versiones que se plasmara en la primera hoja del documento, donde se indica la revisión, la fecha y la modificación.

Se realizará una nueva edición del Manual de Calidad, cuando se produzcan cambios, modificaciones o nuevas versiones en la normativa aplicable.

# CONTROL DE LA INFORMACIÓN DOCUMENTADA.

El Responsable del sistema de Gestión de la Calidad elabora, revisa y distribuye toda la información documentada que afecte a la calidad, para comprobar su idoneidad con los requisitos establecidos en la normativa aplicable, antes de proceder a su distribución. Toda la información documentada, una vez revisada por los responsables de cada área, se sube al gestor documental de la empresa, eManage, y se asocia a cada área y a su vez a cada actividad.

Toda la información documentada, implicada en el cumplimiento de las actividades relacionadas con la Gestión de la Calidad, es controlada y distribuida. Ese control asegura que:

* + - * Se desactive en el menor plazo posible la información documentada obsoleta de todos los puntos de distribución o uso. Las versiones antiguas son sustituidas en eManage sin perder las referencias de grupos, áreas y actividades a las que las versiones antiguas están asignadas.
      * Cualquier información documentada obsoleta retenida por motivos legales o de preservación acordada, esté adecuadamente identificado, la aplicación no elimina tal información, ésta queda en estado inactivo.

Ha de dejarse constancia de la naturaleza del cambio en la información documentada. Dichas modificaciones dan lugar a una nueva edición de la información documentada, dejando constancia de ello en los registros, también indica cual es el procedimiento de subida de información documentada a eManage y quien tiene acceso.

# OPERACIÓN.

# PLANIFICACIÓN Y CONTROL OPERACIONAL:

En este punto se describen los procesos más importantes para llevar a cabo las actividades de Sotec Consulting.

Sotec a través del área comercial, detecta unas necesidades en el mercado que son denominadas por la compañía, oportunidades, que a su vez es una funcionalidad que tenemos ubicada en eManage. Estas oportunidades se gestionan y planifican a través de las distintas unidades de negocio dependiendo del tipo de oportunidad:

* + - Asistencia técnica
    - Proyectos cerrados y servicios gestionados
    - Producto

El flujo completo se lleva a cabo a través de la herramienta eManage, a través de la cual se documentan tanto las necesidades como los requisitos de las partes interesadas.

La metodología a seguir por Sotec Consulting ya sea a nivel comercial como a nivel de prestación de servicios está documentada en los diferentes procedimientos comerciales recogidos en cada unidad de negocio y subidos al gestor documental de eManage.

# DETERMINACIÓN DE LOS REQUISITOS PARA LOS PRODUCTOS Y SERVICIOS.

Una vez determinadas las necesidades del cliente, estas se cotejan con el Offering de servicios para definir las características de la solución a ofertar que serán.

Dichas necesidades son subidas a eManage a través de alta pedido y alta oportunidad. El seguimiento de actualización del flujo se realizara a través de la herramienta en las distintas reuniones de seguimiento comercial:

* + - Reunión de Forecast
    - Reunión de Pipeline
    - Reuniones de seguimiento individuales.
    - Revisión de los requisitos del producto/servicios y solicitados por el cliente

En el caso de los productos, una vez estén creados se pasan por un equipo de testeo, donde se buscan fallos tanto de funcionalidad como de usabilidad. Posteriormente, se genera un informe de dichos fallos y se envía a los responsables del proyecto en sí. Se tratan dichos fallos y se regresa al proceso de testeo hasta que el producto esté correcto.

En el caso de nuestros servicios, si existe una reclamación del cliente y la mejora no existe en nuestro catálogo, se genera un nuevo modelo, se personaliza y lanzamos la oferta de nuevo al cliente.

* + - *Comunicación con el cliente.*

Sotec Consulting tiene establecido un sistema de comunicación continua con las partes interesadas. Este sistema de comunicación se recoge a través de la planificación comercial y de las minutas. Estas últimas se suben al sistema después de cada reunión comercial con la parte interesada.

A la hora de ofertarnos, disponemos de un catálogo de servicios donde expondremos a los clientes nuestros servicios y productos.

Disponemos de un procedimiento circular (workflow) que utilizamos como método principal de entrega y comunicación con el cliente.

# DISEÑO Y DESARROLLO DE LOS PRODUCTOS Y SERVICIOS.

# PLANIFICACIÓN DEL DISEÑO Y DESARROLLO.

A través de nuestra herramienta eManage se solicitan los desarrollos tanto internos de la compañía como externos, es decir, los solicitados por nuestros clientes a través del área comercial. A través de la herramienta, se tiene que indicar quien, cómo y por qué se solicita, se tiene que subir la documentación del funcional y realizar la ponderación comercial:

* + - * La planificación del diseño y desarrollo contemplando las diferentes fases del servicio. Esta planificación será revisada y actualizada tantas veces como sea necesario durante las fases del diseño.
      * Los elementos de entrada para diseño y desarrollo.
      * Resultados del diseño.
      * Verificaciones, validaciones y modificaciones del diseño y desarrollo.
      * Control de los cambios del diseño.

El diseño de los desarrollos realizados a la parte interesada es responsabilidad de éstos.

En la herramienta eManage se recogen los requisitos en “Herramientas/solicitud de desarrollo”

# ELEMENTOS DE ENTRADA PARA EL DISEÑO DE DESARROLLO

Existe un procedimiento en el gestor documental de eManage, en el apartado de comercial, en la actividad CR12 sobre gestión del producto, donde aparece cómo realizar un funcional, que es el instrumento de entrada para el desarrollo del producto.

En la herramienta de solicitud de desarrollos en eManage, se gestionan y desarrollan todas las peticiones en forma de funcional, que recibamos de los clientes.

# CONTROLES DE DISEÑO Y DESARROLLO,

En el gestor documental, en el apartado de Comercial> BU de Producto, aparece un procedimiento de testing, para control el diseño y desarrollo del producto, conforme nuestros requisitos y los requerimientos de los clientes.

# ELEMENTOS DE SALIDA DEL DISEÑO Y DESARROLLO.

En el apartado de eManage de Solicitud de desarrollo, se desarrollará el testeo, conforme al pprocedimiento al que hacemos referencia en el aprtado anterior.

# CAMBIOS EN EL DISEÑO Y DESARROLLO.

En este punto, contamos con un control de versiones tanto en las aplicaciones, como en las modificaciones que se realicen en los documentos.

En el Manual de Cultura Corporativa, que se encuentra disponible para los empleados en la Capacitación de eManage, aparece reflejado como hay que registrar en los documentos la versión y modificación que se ha realizado.

# CONTROL DE LOS PRODUCTOS Y SERVICIOS SUMINISTRADOS EXTERNAMENTE.

# *GENERALIDADES.*

Sotec Consulting ha establecido, implantado y mantiene un Sistema de Gestión de la Calidad y Seguridad de la Información de acuerdo a lo establecido en la **Norma ISO 9001y 27001 correspondiente**, y ha implantado mecanismos para el seguimiento, medición y análisis de los procesos a través de indicadores y ha establecido un compromiso para lograr los resultados planificados y alcanzar la mejora según los datos obtenidos. El ámbito de la aplicación del Sistema de Gestión de la Calidad se centra en la *Consultoría, desarrollo, implantación, integración y mantenimiento de proyectos de tecnologías de la información, negocio y procesos, a través de las diferentes áreas de asistencia técnica, servicios gestionados, diseño y desarrollo de proyectos software y formación.*

# TIPO Y ALCANCE DEL CONTROL DE PROVISIÓN EXTERNA.

Sotec Consulting lleva a cabo principalmente las siguientes compras:

* Equipos e infraestructura necesarios para el desarrollo de la actividad
* Subcontratación de servicios (estudios, consultoría, varios,…)

Sotec Consulting se asegura de que los equipos/servicio comprado/subcontratado cumple con los requisitos establecidos por la parte interesada, para ello selecciona a su parte interesada por su capacidad para cumplir las especificaciones establecidas por la parte interesada.

A fin de comprobar que la parte interesada reúne los requisitos mínimos adecuados para suministrar los bienes y servicios comprados/subcontratados, se establece un proceso denominado AC, Actividades AC31, AC32, AC33 y AC34.

El Responsable de Compras, elabora y mantiene actualizada una Lista de Partes interesadas (pool de proveedores) actividad AC15.

Anualmente se evaluaran o reevaluarán las partes interesadas que han participado en las diferentes operaciones en función de la presencia /ausencia de incidencias/calidad/plazos entrega.

Dicha información se recoge en el área de Compras, en eManage.

A Través de la herramienta eManage, pestaña compras, se pueden llevar a cabo las solicitudes de compras

# INFORMACIÓN PARA LOS PROVEEDORES.

Sotec Consulting tiene por costumbre definir claramente a sus proveedores cuáles son sus requerimientos y standares de calidad requeridos. Estos requerimientos se le expresan en las reuniones planificadas para tal fin, de forma verbal.

# PRODUCCIÓN Y PRESTACIÓN DEL SERVICIO.

# CONTROL DE LA PRODUCCIÓN Y DE LA PROVISIÓN EL SERVICIO

Sotec Consulting tiene **información documentada** sobre las características de los productos, servicios a prestar y actividades a desarrollar, así como los resultados a alcanzar en **eManage**. Esta documentación se encuentra en la pestaña de Comercial>Productos>Consulta de productos y aparece un listado de todos ellos. Dentro de cada producto aparece reflejada toda la información que requiere la norma:

* + - * En cuanto a los servicios, encontramos toda la información requerida en la pestaña de eManage de Comercial>BUL>Consulta BUL. Aparecen reflejado el catálogo de los servicios que prestamos con las características y condiciones de cada uno de ellos.
      * En la misma pestaña, en el apartado de resultados, se refleja la disponibilidad y el uso de los recursos de seguimiento y medición adecuados.

Para la realización del **seguimiento**, en las mismas pestañas existen liturgias de seguimiento. Además, semanalmente tienen lugar las reuniones de Forecast y Pipeline, donde se analiza el estado de los pedidos y los objetivos semanales, así como su evolución y avance. Por último, realizamos unas actividades de seguimiento del resultado de nuestros productos y servicios, a través de reuniones periódicas con el cliente, y del vector posicionamiento que registra anualmente la satisfacción y nuevas peticiones del cliente.

El **entorno** donde están ubicados los procesos y donde quedan reflejados los registros es nuestra herramienta eManage. Tenemos los procedimientos automatización en nuestra plataforma, de tal manera que se puedan evitar posibles errores al realizar nuestras acciones de la manera correcta. En el caso de que exista algún procedimiento poco eficiente, existe la posibilidad de modificarlo, para ir mejorando nuestro modo de trabajar adaptándolo a las nuevas necesidades.

En cuanto a la **designación de personas competentes,** en eManage podemos ver la información de cada empleado en la pestaña de candidatos> consulta. En este apartado podemos ver la formación y experiencia de cada uno, para poder ubicarlos en el puesto adecuado.

# IDENTIFICACIÓN Y TRAZABILIDAD.

Identificamos los productos y servicio en cada una de las fases de nuestro procedimiento de prestación y oferta.

En el caso de los productos, el procedimiento se encuentra recogido en el gestor documental en Comercial en el apartado Producto y la actividad Gestión de productos. En él aparece reflejado como identificar y guardar todos los datos del producto durante todo el procedimiento, desde el inicio de la oportunidad y solicitud de desarrollo, hasta su salida.

En el caso de los servicios, existen procedimientos también en el gestor documental de eManage, en el Grupo Comercial. Cada BU tiene sus procedimientos y sus mediciones y registros del seguimiento del servicio que prestamos.

# PROPIEDAD PERTENECIENTE A LOS CLIENTES O PROVEEDORES EXTERNOS

La única propiedad que tenemos del cliente son sus datos, que son tratados conforme la legislación vigente de Protección de Datos.

En el caso del servicio de consultoría externa o Asistencia Técnica, los recursos humanos aportados son propiedad de Sotec, por lo que se rigen en base a nuestra normativa. No obstante, nuestros clientes nos pueden establecer una serie de obligaciones a incluir en esa prestación de servicios.

En el caso de los Productos ofertados, lo que facilitamos es un acceso al software creado por Sotec Consulting. Por lo tanto, no es propiedad perteneciente a los clientes, si no de nuestra organización.

# PRESERVACIÓN

Todas las condiciones respecto a seguridad, protección, características del producto y prestación de servicio, están documentados en eManage en las respectivas Bus y en el apartado de Solicitud de desarrollo en el caso de los productos.

Garantizamos en los contratos la protección de los datos del cliente, la prestación del servicio, entrega y mantenimiento del producto, en definitiva, el cumplimiento de lo previamente acordado con el cliente.

# ACTIVIDADES POSTERIORES A LA ENTREGA.

Sotec Consulting lleva a cabo la gestión y entrega de los proyectos, servicios de forma controlada. A través de los procedimientos comercial AT, proyecto cerrado, y a actividad Post venta se recoge las tareas que deben realizarse para el control de post venta, procedimentado y documentado en el gestor documental en Comercial> CG Post Venta en las actividades CG01 a CG12

La correcta realización de cada una de las actividades reflejadas en las actividades citadas anteriormente, permite asegurar que el servicio prestado cumplirá con lo especificado en los requisitos de las partes interesadas. En caso contrario, se obtendrán las evidencias necesarias de cuáles han sido las no conformidades detectadas o las reclamaciones recibidas, para poder tomar las decisiones necesarias y conseguir una mejora de los procesos.

# CONTROL DE CAMBIOS.

El control de cambios se lleva a cabo a través de la herramienta eManage, que almacena las versiones anteriores de los documentos ante nuevos cambios.

# LIBERACIÓN DE LOS PRODUCTOS Y SERVICIOS.

Antes de liberar el producto es necesario tener la conformidad de los requisitos por parte del cliente, dicha conformidad puede ser recibida a través de la firma de la oferta presentada al cliente donde se recogen las especificaciones del servicio/ producto o en otros caso vía email, dando el cliente el ok del mismo, o a través de los números de pedido que los clientes emiten para la facturación donde se aceptan las condiciones del servicio/ producto.

Además, tenemos establecido un checklist donde comprobamos que todos los requisitos se han cumplido, cuando se está realizando la fase de testing. Este paso está documentado en eManage, en el gestor documental, en la parte de comercial>Producto, además de registrarse toda la información en la pestaña de solicitud de desarrollo.

# CONTROL DE LOS ELEMENTOS DE SALIDA DEL PROCESO, LOS PRODUCTOS Y SERVICIOS NO CONFORMES.

Existe un correo electrónico destinado especialmente, para comunicarnos las incidencias de los productos que entregamos a los clientes, que por procedimiento se deben solucionar en 24/48 horas. Estas no conformidades aparecerán reflejadas en la herramienta incidencias, para trabajarlas desde ahí y realizar el workflow correspondiente.

En cuanto a los servicios se hace un seguimiento del cliente post venta como bien establecen las actividades ubicadas en eManage en en apartado de Comercial, CG Post venta. Este seguimiento, se queda reflejado en las minutas que realizan los comerciales y que han de subir a eManage.

# EVALUACIÓN DEL DESEMPEÑO.

# SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.

Tanto Dirección como el departamento comercial mantienen un contacto directo con la parte interesada. No obstante, durante la revisión del sistema analiza la percepción de la parte interesada respecto al servicio que prestado por Sotec Consulting:

Es política atender adecuadamente las reclamaciones o sugerencias que la parte interesada puedan formular tanto por escrito como verbalmente, y deben ser canalizadas por el responsable de cada área y a través de la herramienta eManage.

Para ello, deberá quedar registrado como incidencia dentro del Gestor de incidencias de eManage.

Asimismo en la revisión por la dirección se analizan los datos siguientes:

* + - Percepciones y comentarios continuos por parte de la parte interesada.
    - Percepciones del personal de Sotec Consulting.
    - Indicadores comerciales.
    - Indicadores de fidelización.

Del análisis efectuado se determinarán las áreas en las que se necesita mejorar. Esta información servirá a Dirección para establecer los objetivos de la calidad y será tratada como registros de calidad.

Sotec Consulting se compromete a proporcionar los medios y emprender las acciones necesarias que posibiliten suministrar un servicio acorde con las especificaciones requeridas por nuestras partes interesadas. Se planifica e implementa los procesos de seguimiento, medición, análisis y mejora necesarios para:

* + - Demostrar la conformidad del servicio prestado.
    - Asegurarse de la conformidad del Sistema de Gestión de la Calidad.
    - Mejorar la eficacia del Sistema de Gestión de la Calidad.

#### Seguimiento y medición de los procesos:

Se realiza un seguimiento de los procesos que se llevan a cabo, para ello cuenta con la ayuda del resto de los responsables de departamento. Para realizar este seguimiento se dispone de indicadores de los procesos significativos, así como los establecidos en relación a los objetivos fijados y aprobados por Dirección. Cada área tiene unos objetivos de resultados claramente definidos los cuales se analizan en las diferentes reuniones individuales con los responsables.

Para cada uno de los Indicadores KPI, la Dirección de Sotec Consulting, establecerá y aprobará un resultado planificado o umbral mínimo que esperan obtener en un plazo determinado, necesario para la buena marcha de la organización.

# SATISFACCIÓN DEL CLIENTE.

Tanto Dirección como el departamento comercial mantienen un contacto directo con el cliente. Con periodicidad anual se lanzan las encuestas de satisfacción a clientes que son analizadas por el departamento de marketing, y, junto con el estudio de la competencia sirven para identificar líneas de mejora.

También medimos la satisfacción del cliente a través del procedimiento Vector de posicionamiento. Este procedimiento se encuentra ubicado en eManage en el gestor documental en las actividades CA11 Vector posicionamiento por competencia y CA 12 Vector de posicionamiento por cliente.

# ANÁLISIS Y EVALUACIÓN.

Sotec Consulting recopila la información necesaria y los datos apropiados para demostrar la idoneidad y la eficacia del Sistema de Gestión de la Calidad; y para evaluar dónde puede realizarse la mejora de la eficacia del sistema.

En los diferentes análisis que realizamos incluimos:

1. La conformidad de los productos y servicios, partiendo del seguimiento periódico que realizan los comerciales, y de las incidencias reportadas.
2. El grado de satisfacción del cliente, a través de las encuestas de satisfacción anuales y el vector posicionamiento
3. El desempeño y la eficacia del sistema de la calidad, a través del acta de revisión por la dirección
4. Si nuestras implantaciones son eficaces, mediante la medición de los objetivos
5. La eficacia de las acciones tomadas para abordar riesgos y oportunidades, a través del análisis de riesgos, y de las reuniones de Forecast y Pipeline
6. El desempeño de los proveedores externos, a través de nuestra evaluación a los proveedores
7. La necesidad de mejoras en el sistema de gestión de calidad, a través de las acciones correctivas y la herramienta incidencias.

# AUDITORÍA INTERNA.

Sotec Consulting realiza auditorías programadas en función de la naturaleza e importancia de las actividades que van a ser auditadas y son llevadas a cabo por personal independiente de aquellos que tienen la responsabilidad directa en la actividad que vaya a ser auditada. Dicho personal debe cumplir con los requisitos especificados en la ficha de cualificación para el Auditor de Calidad.

La actividad derivada de la auditoría interna, está recogida en la actividad de auditoria interna de todas las ISO, ubicadas en la pestaña Gerente, que se encuentra en el gestor documental de eManage.

Tenemos una planificación anual de todas las auditorias, tanto internas, como las externas. Las auditorías se realizarán anualmente y se entregará informe de Auditoría inmediatamente a Dirección.

Todas las no conformidades y observaciones que resulten de la auditoría interna, y de la externa cuando se dé el caso, se reflejan en nuestra herramienta de Incidencias, a través de la cual se tratará la incidencia, se analizará su causa raíz, y quedará cerrada. De esta manera aprovechamos esta fuente de correcciones, como mejora continua.

La dirección responsable del área auditada será la encargada del seguimiento y cierre de las correcciones y las acciones correctivas necesarias sin demora justificada, para eliminar las no conformidades y sus causas.

# REVISIÓN POR LA DIRECCIÓN.

A fin de asegurar la eficacia y la eficiencia del Sistema de Gestión de la Calidad y la aplicación de la política, el Responsable del sistema de Gestión de la Calidad junto con la Dirección, se reúnen al menos una vez por año para revisar el sistema implantado.

# ENTRADAS DE LA REVISIÓN POR LA DIRECCIÓN.

Esta revisión se realiza por medio del procedimiento establecido y documentado en la actividad de Revisión por la dirección de Gerencia en el gestor documental de eManage. Es documentada mediante un Acta de Revisión por la dirección, el cual se habrá de rellenar mediante una plantilla, donde se tratarán al menos los siguientes puntos:

* + - 1. Revisión del estado de las acciones de revisiones anteriores.
      2. Estado de los cambios en las cuestiones externas e internas.
      3. Grado de cumplimiento de los objetivos.
      4. Análisis del desempeño y eficacia del sistema de gestión.
      5. Nivel de adecuación de los recursos.
      6. Grado de eficacia de las acciones para abordar riesgos y oportunidades
      7. Revisión de las comunicaciones con las partes interesada.
      8. Oportunidades de mejora continua

# SALIDAS DE LA REVISIÓN POR LA DIRECCIÓN.

A través de ese informe se sacan unas conclusiones y unas acciones para evitar los posibles fallos que hayan surgido, y para continuar con la mejora continua de la compañía.

Se estudiarán las oportunidades mejora, la necesidad de cambios en los sistemas de gestión, así como de la necesidad y asignación de recursos.

# MEJORA.

# GENERALIDADES

Sotec Consulting, basa su sistema de gestión en la mejora continua, por lo que en cada incidencia o no conformidad en cualquier área de nuestro trabajo, lo enfocamos como una oportunidad de mejora y avance en la calidad de la compañía.

# NO CONFORMIDAD Y ACCIÓN CORRECTIVA.

La Dirección, a través de los seguimientos periódicos, auditorías y revisiones, evalúa y mide la evolución de la compañía, y las no conformidades e incidencias que puedan surgir.

Para ellos, tenemos establecido en eManage la herramienta de **Incidencias**, a través de la cual gestionamos todas las no conformidades o errores que puedan darse en la compañía. Cualquier persona puede subir una incidencia, para mejorar cualquier aspecto que haya detectado que ha fallado en el procedimiento.

Para la gestión de las Incidencias, se sigue la metodología GROW, consistente en 4 fases. La primera “Goal” donde se define el objetivo; la segunda “Reality” donde se analiza la realidad; la tercera “Options” donde se analizan las alternativas; y por último “Will” que será el plan de acción.

El objetivo de esto es:

* + - La solución de los problemas que causan desviaciones del Sistema de Gestión.
    - Establecer las responsabilidades para controlar e investigar las no conformidades reales o potenciales y desarrollar las acciones correctivas o preventivas correspondientes.
    - La aplicación de controles para garantizar la eficacia de las acciones correctivas.
    - El uso de todas las fuentes de información de la empresa para detectar, analizar y eliminar las causas de las no conformidades.
    - La determinación de los pasos necesarios para implantar acciones correctivas.
    - La información a Dirección sobre las acciones realizadas a efectos de revisión.

#### - Acción correctiva:

Una situación de deficiencia con respecto a la calidad puede detectarse como consecuencia del resultado de una auditoría interna o externa, en el transcurso de una revisión, por reclamaciones, incidencias de partes interesadas, etc.

Una vez detectadas se requiere un estudio para determinar las causas que las motivaron. Las acciones correctivas tomadas para eliminar las causas de las no conformidades reales o potenciales son proporcionales a la magnitud de los problemas detectados y a los riesgos que de ellos puedan derivarse. Todas esas acciones se documentan en el Gestor de Incidencias de eManage.

El Responsable del sistema de Gestión de la Calidad verifica la correcta implantación de las acciones correctivas aprobadas, indicando la información documentada relacionada con el contrato, o bien las medidas adaptadas para la solución de la causa, en los procesos o en el Sistema de Gestión de la Calidad.

# MEJORA CONTINUA.

Sotec Consulting en su empeño por mejorar la eficacia del Sistema emplea las siguientes herramientas:

* + - La Política de la Calidad: revisándola y manteniéndola al día.
    - Los Objetivos de Calidad: satisfaciendo las metas propuestas y analizando los resultados alcanzados.
    - Las auditorías internas/externas: obteniendo información sobre la implementación y eficacia del Sistema.
    - Análisis de los datos: recopilando información de los procesos que componen la empresa.
    - Las acciones correctivas: eliminando la causa de las no conformidades detectadas.
    - La revisión por la Dirección y las reuniones periódicas de la Dirección/Comercial/Administración.

# SEGURIDAD DE LA INFORMACIÓN

El Responsable de la Seguridad de la información y el de Calidad trabajan conjuntamente en el desarrollo del presente manual y control de Anexo para tener integrado los dos sistemas.

Como documentos adicionales a este Manual se han generado los siguientes Documentos que están ubicados en el grupo de Gerentes, tarea GR\_ISO.

PSI-01 Valoración del Riesgo.



PSI-02 Reutilización y destrucción de soportes y equipos. PSI-03 Procedimiento de Backup.

PSI-04 Plan de Contingencia.

# POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

# DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

# CONTROL A.5.1.1. Políticas para la Seguridad de la Información

La Dirección de **SOTEC** reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, divulgación, modificación y la utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, manuales, casos de estudio, códigos fuente, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

Es política de **SOTEC** que:

* + - 1. Se establezcan anualmente objetivos con relación a la Seguridad de la Información.
      2. Se desarrolle un proceso de análisis del riesgo y de acuerdo a su resultado, se implementen las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables.
      3. Se establezcan los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgos surjan del proceso de Análisis de riesgos manejado.
      4. Se cumpla con los requisitos del negocio, legales o reglamentarios y las obligaciones contractuales de seguridad.
      5. Se brinde concienciación y entrenamiento en materia de seguridad de la información a todo el personal.
      6. Se establezcan los medios necesarios para garantizar la continuidad del negocio de la empresa.
      7. Se sancione cualquier violación a esta política o a cualquier política/procedimiento del SGSI.
      8. Todo empleado es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas.
      9. Todo empleado es responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política y de las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.
      10. El Departamento de Calidad y de Operaciones es responsable directo sobre el mantenimiento de esta política, por brindar consejo y guía para su implementación, e investigar toda violación reportada por el personal.

# CONTROL A.5.1.2 Revisión de las políticas para la Seguridad de la Información

Anualmente se revisarán las políticas para la seguridad de la información siempre que haya cambios significativos y se marcarán los objetivos del año junto con la Dirección, que quedará reflejado en la auditoría interna.

# ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

# ORGANIZACIÓN INTERNA

# CONTROL A.6.1.1 Roles y Responsabilidades de la Seguridad de la información.

Responsabilidades, velar por la seguridad. Revisión de controles, actualización del SGSI. Revisión de procesos relacionados con SGSI y actualización. Objetivos de Seguridad de la información y evaluación de los riesgos.

Estas responsabilidades se asignan al responsable del depto. de Operaciones.

# CONTROL A.6.1.2 Segregación de tareas.

La Compañía se estructura para que la información no recaiga en una única persona. La segregación de tareas se ve reflejado en el organigrama de la empresa.

Cada persona tiene asignado un rol con acceso limitado a sus funciones en base a sus responsabilidades. Todo el acceso a documentación, está controlado en el ERP eManage. El rol superadmin que se lo posee dos personas de la compañía son los que controlan el acceso a eManage. Una de ellas el responsable de SGSI y otra el responsable de administración.

# CONTROL A.6.1.3 Contacto con Autoridades.

Departamento Jurídico. Checklist de seguimiento jurídico, pestaña con los contactos. Se mantienen comunicaciones con INCIBE (instituto nacional de cyberseguridad).

# CONTROL A.6.1.4 Contacto con grupos de especial interés.

Sotec Consulting consta de un Pool de colaboradores externos y proveedores, incluyendo abogados en Protección de datos, Propiedad industrial e intelectual, así como entidades subcontratadas de Prevención de Riesgos Laborales (MGO y LOPD).

# CONTROL A.6.1.5 Seguridad de la Información en la gestión de proyectos.

Referenciado al Documento “Procedimiento de Operaciones”.

Grupo Operaciones. Capacitación operaciones. OA01 Procedimiento.

# DISPOSITIVOS MÓVILES Y TELETRABAJO

# CONTROL A.6.2.1 Política de dispositivos móviles.

 Manual de uso y gestión de dispositivos

 Documento entrega y devolución de dispositivos

 Plantilla baja trabajador recordatorio de cláusulas.

# CONTROL A.6.2.2 Teletrabajo.

* No aplica, ningún trabajador ejercita sus labores desde un emplazamiento diferente a las oficinas de Sotec. Excepto en el caso tipificado en el plan de contingencia derivado del Riesgo Edificio/Local.

# SEGURIDAD LIGADA A RECURSOS HUMANOS

# ANTES DEL EMPLEO

# CONTROL A.7.1.1 Investigación de antecedentes.

 Al publicarse ofertas a través de portales con los que tenemos firmados contratos y en cuyos portales figuran las cláusulas que lo rigen, hemos de cumplir los requisitos exigidos al publicar las ofertas, en caso contrario nos eliminarían la oferta. Si la búsqueda de empleo se lleva a cabo por CV recibidos en nuestra página web. podemos comprobar accediendo a [www.sotec.es](http://www.sotec.es/) que están los términos legales, condiciones de uso y alusiones a PRL al subir los CV.

Manual de conducta. (Código éticos y valores de la empresa).

 Manual de bienvenida (Código éticos y valores de la empresa).

# CONTROL A.7.1.2 Términos y Condiciones de Empleo.

 Procedimiento de Administracion. En el que se fija la gestión del alta del trabajador y todos los documentos que deberá firmar y entregársele.

 Cláusulas anexas a los contratos de trabajadores.

 Procedimiento de Administración donde se contempla la existencia y el fin de acuerdos NDA.

 Código de conducta. En el "punto de desempeño" se marca y exige confidencialidad y uso de documentos.

# DURANTE EL EMPLEO

# CONTROL A.7.2.1 Responsabilidades de Gestión.

 Código de conducta. En el "punto de desempeño" se marca y exige confidencialidad y uso de documentos

 Manual de bienvenida. Alude a prevención de riesgos laborales y confidencialidad además de la política entera de valores de SOTEC.

 Procedimiento de capacitación en el que se capacita desde las diferentes áreas de la empresa y entre ellas, desde administracion sobre LOPD y PRL

 Procedimiento y manual de LOPD y MGO sobre prevención de riesgos laborales y LOPD.

# CONTROL A.7.2.2 Concienciación, educación y capacitación en Seguridad de la Información.

 Código de conducta. En el "punto de desempeño" se marca y exige confidencialidad y uso de documentos.

 Manual de bienvenida. Alude a prevención de riesgos laborales y confidencialidad además de la política entera de valores de SOTEC.\_\_Procedimiento de capacitación en el que se capacita desde las diferentes áreas de la empresa y entre ellas, desde administracion sobre LOPD y PRL

 Procedimiento y manual de LOPD y MGO sobre prevención de riesgos laborales y LOPD.

 El responsable del área actualizará los documentos de capacitación y realizará exámenes periódicos cuando haya alguna actualización.

# CONTROL A.7.2.3 Proceso disciplinario.

 Implantando un sistema disciplinario de infracciones y sanciones. Documento en eManage.

 Documentos entregados a trabajadores sobre PRL.



# FINALIZACIÓN O CESE DEL EMPLEO

# CONTROL A.7.3.1 Responsabilidades ante la finalización o cambio.

 Plantilla baja trabajador recordatorio de cláusulas (Administracion 2012/Sotec-HRT/Laboral/documentación bajas/España/recordatorio de clausulas plantilla.)

 Para los trabajadores del departamento de operaciones tienen unas clausulas especiales recordando la propiedad intelectual e industrial.

 Documento de devolución de móvil y portátil

 En la capacitación de administración y actividades de depto. de laboral se describe la actuación de Administracion una vez que se recibe la baja de un trabajador.

# GESTIÓN DE ACTIVOS

# RESPONSABILIDAD DE LOS ACTIVOS

# CONTROL A.8.1.1 Inventario de los Activos.

 Desarrollo propio en eManage. Sistema  Control de dispositivos

# CONTROL A.8.1.2 Propiedad de los Activos.

 Desarrollo propio en eManage. Sistema  Control de dispositivos

# CONTROL A.8.1.3 Uso aceptable de los activos.

 Documento de entrega y devolución de móvil y portátil (Administracion/Administracion 2012/sotec-hrt/móviles y portátiles/plantillas)

 Documento de recepción de Pack de Bienvenida En la última frase hay un recibí de entrega y aceptación.

 Cláusulas anexas a los contratos de trabajadores [(Administración/Administracion 2012/Sotec-HRT/Contratos mercantiles/Plantillas/Contrato/Clausulas adicionales(La 1 y la 4)]

 Manual de uso y gestión de dispositivos

# CONTROL A.8.1.4 Devolución de Activos.

 Documento de entrega y devolución de móvil y portátil (Administracion/Administracion 2012/sotec-hrt/móviles y portátiles/plantillas)

 Cláusulas anexas a los contratos de trabajadores [(Administración/Administración 2012/Sotec-HRT/Contratos mercantiles/Plantillas/Contrato/Clausulas adicionales(La 1 y la 4)]

 Plantilla baja trabajador recordatorio de cláusulas (Administración 2012/Sotec-HRT/Cartas/Plantillas/doc.)

# CLASIFICACIÓN DE LA INFORMACIÓN

# CONTROL A.8.2.1 Clasificación de la información.

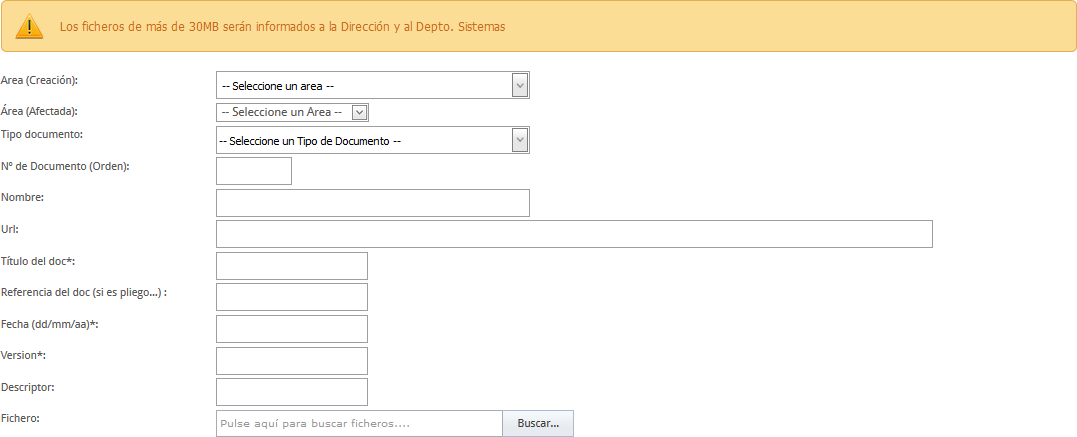
 A nivel externo, RAPINFORMES (Empresa subcontratada para Protección de datos) Documentos entregados a trabajadores sobre PRL y LOPD.

 A nivel interno mediante Roles y grupos en herramienta eManage, diferentes permisos en función del perfil en la compañía.

Documento tratamiento de la información.

# CONTROL A.8.2.2 Etiquetado de la información.

Etiquetar la documentación. Mediante los descriptores en la subida de documentación.



# CONTROL A.8.2.3 Manipulado de la información.

 Cláusulas anexas a los contratos de trabajadores [(Administración/Administracion 2012/Sotec-HRT/Contratos mercantiles/Plantillas/Contrato/Clausulas adicionales(La 1 y la 4)]

 Código de conducta. En el "punto de desempeño" se marca y exige confidencialidad y uso de documentos.

 Sistema disciplinario.

# MANIPULACIÓN DE LOS SOPORTES

# CONTROL A.8.3.1 Gestión de dispositivos extraíbles.

Llamamos como dispositivos extraíbles cualquier dispositivo que se conecte a un pc.

* + - * Moviles, está permitida la conexión de móviles a los ordenadores siempre y cuando sea para la carga del mismo, para ello en sistemas Android hay que habilitar la opción de sólo carga, se hace mención a ello en el Manual de uso y gestión de dispositivos.
      * Tablets, ídem que los móviles.
      * PenDrives, no está permitido el uso de pendrives excepto el personal del departamento de operaciones.
      * Discos duros extraíbles, en ordenadores críticos, administración, comercial, cada ordenador tiene un disco duro extraíble, que se utilizará para back ups.

# CONTROL A.8.3.2 Retirada de soportes físicos.

PSI-02 REUTILIZACIÓN Y DESTRUCCIÓN DE SOPORTES Y EQUIPOS.

# CONTROL A.8.3.3 Soportes físicos en tránsito (Transporte de elementos).

Todos los documentos que contienen información relevante para la compañía se encuentran dentro de la herramienta de gestión de documentación en eManage. Para el acceso a esta herramienta los usuarios deben introducir usuario y contraseña. Para el resto de documentos de los ordenadores con información relevante están protegidos por contraseña, como es el caso del fichero de contraseñas de correo, servidores, este fichero está protegido por contraseña.

# CONTROL DE ACCESO

# REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

# CONTROL A.9.1.1 Política de Control de acceso.

El acceso de la información en eManage está controlado por Roles de acceso que permiten el acceso a opciones del Menú, así como por usuario y contraseña.

El detalle de los Roles y a qué tiene acceso cada persona lo gestiona operaciones.

El acceso a las oficinas está controlado por alarma y al edificio por video vigilancia y portero físico. Las personas que poseen llaves de las oficinas, son dos por cada oficina, previa firma de documento de cesión de llaves y control de dispositivos en eManage.

# CONTROL A.9.1.2 Acceso a redes y servicios en red.

Procedimiento de operaciones.

Servicio en red: eManage: El acceso a la aplicación eManage se realiza por contraseña y ésta no puede ser igual a las 5 últimas. La contraseña debe tener al menos 8 caracteres y a los 3 intentos fallidos se bloquea.

e-time: La contraseña de acceso a e-time se gestiona desde eManage, es decir, en eManage Administración gestiona la contraseña de acceso a e-time.

# GESTION DE ACCESOS DE USUARIOS

# CONTROL A.9.2.1 Registro y baja de usuarios.

 El depto.. de operaciones recibe notificación con baja de usuario y el mismo departamento realiza la baja en ERP, cuenta de correo (redirección), cuenta de Skype y dispositivos móviles.

# CONTROL A.9.2.2 Provisión de acceso a usuario.

 Manual de uso y gestión de dispositivos.

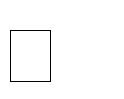
 Gestión de Roles y perfiles en eManage.

# CONTROL A.9.2.3 Gestión de privilegios de acceso (Administradores).

 Manual de uso y gestión de dispositivos.

 Procedimiento de operaciones, acceso a redes.

# CONTROL A.9.2.4 Gestión de autenticaciones de usuarios.

Proceso automatizado de eManage de cambio de contraseña bimensual.

# CONTROL A.9.2.5 Revisión de los derechos de acceso de los usuarios.

El acceso a eManage se realiza desde el Departamento de Operaciones.

# CONTROL A.9.2.6 Retirada o reasignación de los derechos de acceso de los usuarios.

 Check-list de salidas, incluye baja de usuario en eManage.

 Las bajas de los usuarios son comunicadas al depto. de operaciones mediante correo electronico.

# RESPONSABILIDADES DE LOS USUARIOS

# CONTROL A.9.3.1 Uso de contraseñas por parte de los usuarios

Todo empleado debe responsabilizarse que las contraseñas que Sotec Consulting les proporciona sean de carácter personal e intransferible.

Por tanto, está terminantemente prohibido:

* + - * Comunicar a otras personas ya sean internas o ajenas a la organización su usuario y contraseña.
      * Dejar por escrito en un lugar visible, encima de la mesa, el usuario y contraseña.
      * “Prestar” el usuario y contraseña a otro compañero.

# CONTROL DE ACCESOS A APLICACIONES Y SISTEMAS

# CONTROL A.9.4.1 Restricción del acceso a la información.

 Manual de uso y gestión de dispositivos.

 Procedimiento de Administración. En el que se fija la gestión del alta del trabajador en las aplicaciones y en que nos basamos para dárseles de alta.

 El acceso de la información en eManage está controlado por Roles de acceso que permiten el acceso a opciones del Menú. El detalle de los Roles y que puede ver cada uno te lo gestiona el Departamento de administración

# CONTROL A.9.4.2 Procedimiento seguros de inicio de sesión.

Incluido en el procedimiento del Departamento de Administración. En resumen, es lo siguiente:

 EManage: El acceso a la aplicación eManage se realiza por contraseña y esta no puede ser igual a las 5 Últimas. La contraseña debe tener almenas 8 caracteres y a los 3 intentos fallidos se bloquea.

e-time. La contraseña de acceso a e-time se gestiona desde e-Manage, es decir, en eManage se pone la contraseña de acceso a e-time y es administración el encargado de realizarlo.



# CONTROL A.9.4.3 Sistema de gestión de contraseñas.

REFERENCIADO E INCLUIDO EN EL PUNTO A.9.4.2 Procedimiento seguros de inicio de sesión.

# CONTROL A.9.4.4 Uso de utilidades con privilegios del sistema.

Referenciado al plan de contingencia.

# CONTROL A.9.4.5 Control de acceso al código fuente de aplicaciones.

Mediante la herramienta SVN, cada desarrollador dispone de una rama para el desarrollo, una vez que el desarrollador finaliza su trabajo es responsabilidad del PMO, juntar todos los desarrollos (merge) y compilar. Mediante la compilación el código fuente únicamente se ubica en la rama de producción con acceso del PMO y del responsable del dpto. de Operaciones.

# CRIPTOGRAFÍA

# CONTROLES CRIPTOGRÁFICOS

# CONTROL A.10.1.1 Política de uso de controles criptográficos.

No Aplica. Tenemos la posibilidad de que a los documentos de la compañía a los que se les quiere dotar de una seguridad adicional, (documentación de especial relevancia enviada a clientes, propuestas de la compañía...) se protegen mediante marcas de agua.

Consideramos este medio de protección más sencillo de aplicar puesto que en la compañía poseemos una Unidad de Negocio encargada de la comercialización de este sistema de protección de documentos.

# CONTROL A.10.1.2 Gestión de claves para el uso de controles criptográficos

No Aplica. Al no utilizar controles criptográficos no es necesario una gestión de claves para el uso de dichos controles.

# SEGURIDAD FÍSICA Y AMBIENTAL

# ÁREAS SEGURAS

# CONTROL A.11.1.1 Perímetro de seguridad física.

No tenemos CPD. No tenemos áreas. El edificio está dotado con video vigilancia. Las plantas de operaciones y administración, son independientes, securizadas mediante alarma y llave.

# CONTROL A.11.1.2 Controles físicos de entrada.

 Las llaves solo las tienen 2 personas por planta en la empresa y controladas por dirección.

 Sistema de alarma.

 El edificio consta de sistema de videocámara.

 Porteros automáticos con videocámara.

# CONTROL A.11.1.3 Seguridad en oficinas, despachos e instalaciones.

 Las llaves solo las tienen 2 personas por planta en la empresa y controladas por dirección.

 Sistema de alarma.

 Sistema de videocámara.

# CONTROL A.11.1.4 Protecciones frente a amenazas externas y ambientales.

El edificio cuenta con extintores antiincendios situados en los rellanos de cada planta. También se posee de un extintor en cada planta.

# CONTROL A.11.1.5 Trabajo en Áreas seguras (bunker).

No Aplica. A pesar de que se separan (diferentes plantas del edificio) las áreas de Administración y Operaciones del área de negocio para la mejor protección de la información. No contamos con lo que se denominan Áreas seguras (bunker), por lo que no se ha establecido ningún protocolo de trabajo dentro de este tipo de infraestructuras.

# CONTROL A.11.1.6 Áreas de acceso público (recepción, carga y descarga)

No Aplica. **SOTEC** no dispone de una zona de carga y descarga. Además, los proveedores y clientes que visitan las instalaciones son siempre citados por personal de la compañía, cada cliente o proveedor es acompañado por el personal de **SOTEC** que lo ha citado.

La compañía hace responsable al citador del control y supervisión de la persona citada desde su entrada hasta su salida.

# SEGURIDAD DE LOS EQUIPOS

# CONTROL A.11.2.1 Emplazamiento y protección de equipos

El cableado y la protección de equipos son los normales dentro de una organización, el cableado en la medida de lo posible se realiza por canaleta dentro de la pared. En el caso de switches los cables de red no tienen más opción que estar a la vista. Existen switches en las distintas plantas para proporcionar conexión de datos a todos los empleados.

# CONTROL A.11.2.2 Instalaciones de suministro.

Batería propia de los portátiles. Plan de Contingencia.

# CONTROL A.11.2.3 Seguridad del cableado

La seguridad de la red está físicamente separada cada planta y no hay fuentes de agua cercanas, el cableado se mantiene lo más saneado posible, no estando a la vista los switches ni los routes.

# CONTROL A.11.2.4 Mantenimiento de equipos

Gestor de incidencias eManage donde se recogen todas las incidencias relativas al uso de los dispositivos y en el documento PSI-02 Reutilizacion y destrucción de soportes y equipos.

# CONTROL A.11.2.5 Retirada de materiales propiedad de la empresa.

Manual de uso y gestión de dispositivos. Se adjunta a la capacitación común de todos los empleados.

# CONTROL A.11.2.6 Seguridad de los equipos fuera de las instalaciones.

Información adicional en Manual de uso y gestión de dispositivos.

Los equipos están securizados por contraseña si salen fuera de las instalaciones es la manera de securizarlos.

Los teléfonos móviles están securizados mediante pin.

# CONTROL A.11.2.7 Reutilización o retirada segura de equipos.

Documento PSI-02 Reutilización y destrucción de soportes y equipos.

# CONTROL A.11.2.8 Equipos de usuario desatendidos.

Los portátiles de Administración tienen contraseñas individualizadas las cuales se solicitan cada 10 minutos en caso de no hacer uso de los portátiles. Además, se accede a una red ubicada en uno de los portátiles por medio de contraseña cada vez que se accede a esa carpeta. En la medida de lo posible cuando el usuario no atiende a su equipo éste se dejará bloqueado.

# CONTROL A.11.2.9 Política de pantalla y escritorios limpios.

Pack de bienvenida. Servicio de limpieza diario.

# SEGURIDAD EN LAS OPERACIONES

# PROCEDIMIENTOS Y RESPONSABILIDADES DE LAS OPERACIONES

# CONTROL A.12.1.1 Documentación de los procedimientos de Operación.

Procedimiento de operaciones, en este documento se refleja cómo debe ser la documentación relativa a las operaciones.

# CONTROL A.12.1.2 Gestión de Cambios.

Procedimiento de operaciones.

# CONTROL A.12.1.3 Gestión de la Capacidad.

Procedimiento de operaciones.

# CONTROL A.12.1.4 Segregación de los entornos de desarrollo, prueba y producción.

Procedimiento de operaciones (Servidor de Desarrollo).

# PROTECCIÓN CONTRA CÓDIGO MALICIOSO (MALWARE)

# CONTROL A.12.2.1 Controles contra código malicioso.

# DEFINICIONES

Virus informático: es un programa que se copia automáticamente que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso ni el conocimiento del usuario. Aunque popularmente se incluye al "malware" dentro de los virus, en el sentido estricto de esta ciencia los virus son programas que se replican y ejecutan por sí mismos.

Malware: (del inglés malicious software, también llamado badware o Software malicioso): es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento e su dueño. Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso los bots.

Gusano: Son programas similares a los virus, pero los gusanos no dependen de archivos portadores para poder contaminar otros sistemas. Estos pueden modificar el sistema operativo con el fin de auto ejecutarse como parte del proceso de inicialización del sistema. Para contaminar otros sistemas, los gusanos explotan vulnerabilidades.

Troyano: (también llamado caballo de troya) es una pieza de software Dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de Replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador. Su nombre es dado por su peculiar forma de actuar como los Troyanos de la historia, entrando en la computadora, ocultos en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas a la computadora al desarrollar la acción de estos archivos infecciosos.

Spyware: son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Contra estas invasiones, disponemos de un antivirus Avast instalado en todos los ordenadores, debidamente actualizado por cada usuario y revisado aleatoriamente por el depto. de operaciones. Así como en la capacitación común disponemos de dípticos para la formación sobre distintos ataques posibles de virus, spyware, phising.

# OBJETIVO

* + - * Concienciar a los usuarios de los peligros que puede ocasionar el software malicioso.
      * Explicar la importancia de analizar cualquier soporte de datos no fiable (de procedencia incierta, o salido de una red no fiable, adjuntos de correo electrónico). con un software antivirus.
      * Formar a los usuarios en el uso de la herramientas antivirus, útiles para su uso sobre soportes y equipos cuando las medidas centrales no sean de aplicación:

1. Realizar análisis.
2. Configuración de agente activo o Gestión de alertas antivirus.
3. Mantener actualizado el software antivirus.

# PROCEDIMIENTO DE INFORME DE INCIDENCIAS POR SOFTWARE MALICIOSO

El usuario es el encargado de notificar las posibles incidencias relacionadas con el Software malicioso que pueda identificar en soporte o equipos. En el caso que se tenga que hacer alguna notificación se debe registrar en eManage en el Gestor de Incidencias.

# REGISTROS

Quedan todos registrados en el Gestor de Incidencias/no conformes de eManage, incluida su resolución

# COPIAS DE SEGURIDAD

# CONTROL A.12.3.1 Copias de seguridad de la información.

PSI-03 Procedimiento de backup.

# REGISTRO DE EVENTOS Y MONITORIZACIÓN

# CONTROL A.12.4.1 Registro de eventos.

Se monitorizan los backup's OK o KO enviando mails automáticos al Departamento de operaciones ([operaciones@sotec.es](mailto:operaciones@sotec.es))

# CONTROL A.12.4.2 Protección de la información de registro.

Los registros se guardan en el ERP interno, toda documentación, debidamente categorizada y asignada a cada grupo, donde se da acceso a cada usuario. Por lo que la documentación la ve y accede las personas autorizadas para ello.

# CONTROL A.12.4.3 Registros de Administración y Operación.

En la herramienta de registro de incidencias de eManage es donde se recogen todos los registros.

Así como en base de datos del ERP en los datos críticos se recoge la última acción realizada, quien y cuando.

# CONTROL A.12.4.4 Sincronización del reloj.

Los servidores están sincronizados con time.windows.com. Respecto a los usuarios al no tener servidor de dominio no podemos sincronizarlo contra el servidor y no tenemos configurado la sincronización contra un servidor NTP.

# CONTROL DE SOFTWARE EN EXPLOTACIÓN

# CONTROL A.12.5.1 Instalación de software en sistemas de operación.

No entregamos software propio a clientes. Damos acceso a dicho software

# GESTIÓN DE LA VULNERABILIDAD TÉCNICA

# CONTROL A.12.6.1 Gestión de vulnerabilidades técnicas.

Análisis de Riesgos

# CONTROL A.12.6.2 Restricciones a la instalación de software.

Capacitación común. Manual de uso y gestión de dispositivos.

# CONSIDERACIONES A LAS AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

# CONTROL A.12.7.1 Controles de auditoría de Sistemas de la Información.

Auditoría interna. Periocidad anual. Auditoria anual LOPD.

# SEGURIDAD EN LAS COMUNICACIONES

# GESTIÓN DE LA SEGURIDAD DE LA RED

# CONTROL A.13.1.1 Controles de red.

El acceso al Servidor de Producción solo la realiza el responsable del departamento de operaciones.

El acceso a los equipos de la red, está configurada como una red de trabajo en grupo, que cada PC gestiona sus accesos. El acceso a red esta diferenciado entre la 3ª y 5ª Planta y 2ª planta de la escalera Izq.

# CONTROL A.13.1.2 Seguridad de los servicios de red.

En la actualidad tenemos el acceso a red en Madrid contratado con Movistar con FFTH, con el nivel de servicio estándar de Movistar.

El acceso WIFI, se realiza mediante encriptación WPA, que trimestralmente se cambia la contraseña de los puntos de acceso.

# CONTROL A.13.1.3 Segregación de redes.

Los consultores tienen acceso a red desde la ubicación de **SOTEC**, es desde las distintas ubicaciones de los clientes, el acceso a la información de **SOTEC**, se realiza mediante aplicación web son usuario y contraseña.

Tenemos actualmente tres redes segregadas entre los departamentos de la 2ª, 3º y 5ª Planta, no siendo visibles entre ellas.

# INTERCAMBIO DE INFORMACIÓN

# CONTROL A.13.2.1 Políticas y procedimientos de transferencia de información.

Documentos de confidencialidad. Procedimiento jurídico y legal.

Por procedimiento, toda empresa, proveedor, persona física que nos preste algún servicio deberá firmar un contrato de confidencialidad con **SOTEC**. Estos contratos:

 PLANTILLAS (Administracion/Administracion 2012/sotec-hrt/contratos clientes y proveedores/nda/plantillas)

 FIRMADOS: En soporte informático. eManage. En físico guardado en administración.

# CONTROL A.13.2.2 Acuerdos de intercambio de información.

Documentos de confidencialidad. Procedimiento jurídico y legal.

Por procedimiento, toda empresa, proveedor, persona física que nos preste algún servicio deberá firmar un contrato de confidencialidad con SOTEC. Estos contratratos:

 PLANTILLAS (Administracion/Administracion 2012/sotec-hrt/contratos clientes y proveedores/nda/plantillas)

 FIRMADOS: En soporte informático. eManage. En físico guardado en administración.

 En el caso de desarrollo de software poseemos la herramienta SVN con control de usuarios y contraseñas.

# CONTROL A.13.2.3 Mensajería electrónica

Todas las cuentas de correo poseen usuario y contraseña y un único administrador de cuentas. Respecto a los teléfonos móviles, el correo electrónico también posee usuario y contraseña. Las comunicaciones siguen los protocolos de seguridad de los proveedores.

# CONTROL A.13.2.4 Acuerdos de confidencialidad o no divulgación.

 Documentos de confidencialidad. Procedimiento jurídico y legal. Por procedimiento, toda empresa, proveedor, persona física que nos preste algún servicio deberá firmar un contrato de confidencialidad con **SOTEC**. Previa la firma de cualquier contrato de confidencialidad se hace una revisión del mismo por parte del dpto. legal de **SOTEC**.

 CONTRATOS NDA: Estos contratratos: o PLANTILLAS en eManage

o FIRMADOS: En soporte informatico. eManage.

 CONTRATOS MARCO CON CLAUSULAS DE CONFIDENCIALIDAD.

# ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE LA INFORMACIÓN

# REQUISITOS DE SEGURIDAD PARA LOS SISTEMAS DE INFORMACIÓN

# CONTROL A.14.1.1 Análisis y especificación de requisitos de seguridad de la información.

Todos los equipos de desarrollo tienen clave de acceso así como el servidor de desarrollo. Es requisito indispensable que todos poseen claves de acceso. Así como el acceso a la zona de desarrollo será restringida, si fuese necesario acceder será mediante cita previa y acompañado siempre del responsable del departamento.

# CONTROL A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas

Todos los servicios en los que intervienen aplicaciones ubicadas en redes públicas se aseguran mediante certificado SSL, garantizando así la protección de los datos que contienen dichas aplicaciones.

# CONTROL A.14.1.3 Protección de las transacciones de servicios de aplicaciones.

Todos los servicios en los que intervienen aplicaciones ubicadas en redes públicas se aseguran mediante certificado SSL, garantizando así la protección de los datos que contienen dichas aplicaciones.

# SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTCONTROL A.14.2.1 Política para el desarrollo seguro.

Realizamos un desarrollo seguro, en nuestras instalaciones ya que no hay salidas de código, nuestras fuentes se guardan en un servidor seguro en cloud con control de versiones y acceso mediante usuario y contraseña.

# CONTROL A.14.2.2 Procedimientos para el control de cambios en los sistemas.

Control de versiones, con el programa SVN Tortoisse, en este programa se registran todos los cambio de versiones realizadas en el software.

# CONTROL A.14.2.3 Revisión técnica de aplicaciones tras cambios en la plataforma de operación.

Procedimiento de operaciones. “Subida a producción”.

# CONTROL A.14.2.4 Restricciones para los cambios de paquetes de software.

Procedimiento de operaciones. Control de versiones (SVN). Y documento de EspecificacionRepositorio

Actualizaciones de software, predefinidas por el equipo de operaciones y ejecutadas una vez analizado el potencial del riesgo de la actualización.

# CONTROL A.14.2.5 Principios para sistemas de ingeniería seguros.

Mediante la herramienta SVN, procedemos a desarrollo seguro, documentación y control de versiones.

# CONTROL A.14.2.6 Entorno seguro de desarrollo.

Mediante la herramienta SVN se realiza el entorno seguro de desarrollo ya que poseemos todos los logs realizados en código, cuando y quien ha realizado los cambios.

# CONTROL A.14.2.7 Externalización del desarrollo.

Herramienta de control SVN. Además previa a la contratación de software externo los recursos contratados firman la correspondiente cláusula de confidencialidad y se les adjunta copia del procedimiento de operaciones con el fin de ajustar el desarrollo a la normativa corporativa.

# CONTROL A.14.2.8 Pruebas de seguridad del sistema.

Aplicamos metodología de desarrollo en cascada para el desarrollo de software. Documento de plan de pruebas y Ejemplo de pruebas.

# CONTROL A.14.2.9 Pruebas de aceptación del sistema.

Después de cualquier desarrollo se realiza el manual de usuario correspondiente, y el examen del mismo. Se sigue el mismo procedimiento si se realiza cualquier actualización de software, manual y examen.

# DATOS DE PRUEBA

# CONTROL A.14.3.1 Protección de los datos de prueba.

Procedimiento de operaciones.

# RELACIÓN CON PROVEEDORES

# SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

# CONTROL A.15.1.1 Política de seguridad de la información en la relaciones con los proveedores.

 Firma de contrato con proveedores.

# CONTROL A.15.1.2 Requisitos de seguridad en contratos con terceros.

 Contrato y clausulas de proveedores.

# CONTROL A.15.1.3 Cadena de suministro de Tecnología de la Información y de las Comunicaciones.

 Sometido a la política de privacidad del proveedor.

# GESTIÓN DE LA ENTREGA DE SERVICIOS DE PROVEEDORES

# CONTROL A.15.2.1 Control y revisión de la provisión de servicios del proveedor.

Evaluacion de proveedores en eManage.

# CONTROL A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor.

Grupo Administración. Tarea AC10, AC14, AC15, AC31, AC32, AC33

# GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

# GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

# CONTROL A.16.1.1 Procedimientos y responsabilidades.

Gestor de incidencias eManage. Todas las incidencias detectadas por los empleados de SOTEC son gestionadas mediante el gestor de incidencias, independientemente de la naturaleza de las mismas. Es decir, cualquier tipo de incidencia relacionada o no con la seguridad de la información se recoge,

documenta y resuelve de manera eficaz y rápida mediante el gestor de incidencias.

# CONTROL A.16.1.2 Notificación de eventos de seguridad de la información.

Workflow del gestor de incidencias. Una vez detectada y documentada la incidencia, eManage envía una notificación al responsable del área que éste a su vez asigna al recurso más competente en la solución de la misma.

# CONTROL A.16.1.3 Notificación de puntos débiles de la seguridad.

Los empleados mediante la herramienta de incidencias en eManage, contratistas, terceras partes mediante cualquier medio de notificación, correo electrónico, llamada....

# CONTROL A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información.

En el gestor de incidencias hay un checkbox para marcar si la incidencia afecta a seguridad de la información.

# CONTROL A.16.1.5 Respuesta ante incidentes de seguridad de la información.

El gestor de incidencias, cuando la incidencia ha sido solventada, envía automáticamente a los involucrados en dicha incidencia un correo electrónico con el resumen de las acciones correctivas llevadas a cabo.

# CONTROL A.16.1.6 Lecciones aprendidas del análisis de incidentes de seguridad.

En la resolución de la incidencia existe un checklist para que la incidencia no se vuelva a repetir en ninguno de los casos.

# CONTROL A.16.1.7 Recopilación de evidencias.

Gestor de incidencias eManage recopila toda la información. En la BBDD, nunca se borra, se activa o desactiva.

# ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

# CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

# CONTROL A.17.1.1 Planificación de la continuidad de la seguridad de la información.

PSI-04 Plan de contingencia.

# CONTROL A.17.1.2 Implantación de la continuidad de la seguridad de la información.

PSI-04 Plan de contingencia.

# CONTROL A.17.1.3 Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información.

Lo gestiona directamente el Departamento de Operaciones mediante auditoría interna anual.

#### 14.2 REDUNDANCIAS

**14.2.1 CONTROL A.17.2.1 Disponibilidad de los recursos de tratamiento de la información.**

PSI-03 Procedimiento de backup y Análisis de Riesgos.

# CUMPLIMIENTO

# CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

# CONTROL A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.

 Se dispone de registro informático de las normas actuales aplicables. Remisión a la carpeta de documentos jurídicos y al procedimiento legal y jurídico (administracion

central/España/Administracion/Herramientas/Procedimiento juridico y legal).

 Ver Documentos en Gestor Documental de eManage.

 Además contamos con un departamento legal en la empresa y asesores jurídicos externos al que pagamos igualas mensuales o por servicios.

# CONTROL A.18.1.2 Derechos de propiedad intelectual (DPI).

 Está incluida una cláusula de propiedad intelectual en los convenios y contratos de las nuevas incorporaciones en SOTEC.

# CONTROL A.18.1.3 Protección de los registros de la organización.

 Documentos contables y no contables guardados en archivo físico por más de 5 años exigidos.

Guardado de contratos en carpetas, copias y originales.

# CONTROL A.18.1.4 Protección y privacidad de la información de carácter personal.

Se dispone en materia de LOPD las debidas inscripciones de ficheros (situados en un folder dentro de la carpeta de LOPD.

# CONTROL A.18.1.5 Regulación de controles criptográficos.

No aplica. **SOTEC** dota de seguridad a los documentos que lo requieren mediante el sistema de marcas de agua, es por eso que no existe una regulación concreta de los controles criptográficos.

# REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN

# CONTROL A.18.2.1 Revisión independiente de la Seguridad de la Información.

El departamento jurídico se encarga de mantener al día la legislación vigente, realizar controles periódicos e informa de ellas al responsable de operaciones. Posteriormente el responsable de operaciones aplica los cambios a nivel legal que fuesen necesarios.

# CONTROL A.18.2.2 Cumplimiento de las políticas y normas de seguridad.

Auditorías internas de las tres ISOs y Auditorías externas de la LOPD.

# CONTROL A.18.2.3 Comprobación del cumplimiento técnico.

El responsable del depto. vela por el cumplimiento de los procesos y procedimientos.

#### ANEXO I: Checklist comprobación puntos de la norma

* Introducción
* Objeto y campo de aplicación
* Referencias normativas
* Contexto de la organización
* Partes interesadas
* Liderazgo y Política
* Planificación riesgos y oportunidades
* Recursos
* Competencia
* Concienciación
* Comunicación
* Operación
* Evaluación del desempeño
* Auditoría interna
* Revisión por la dirección
* Mejora
* Controles

**ANEXO II. Controles Seguridad de la Información**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AUTOR** | **AREA** | **DIVISIÓN** | |  |
|  | | | | |
| Dirección | Calidad | SOTEC | |  |
|  | | | | |
| **HISTORIAL DE CAMBIOS** | | | | |
|  | | | | |
| **VERSIÓN** | **FECHA** | **CAMBIOS** |  |  |
|  | | | | |
| V1.0 | Feb. 2015 | Primera versión |  |  |
|  | | | | |
| V2.0 | Feb. 2015 | Revisión y aprobación | |  |
|  | | | | |
| V3.0 | Feb. 2015 | Revisión y aprobación | |  |
|  | | | | |
| V4.0 | Feb.2016 | Revisión y aprobación | |  |
|  | | | | |
| V5.0 | Mar.2016 | Revisión y rectificación | |  |
|  | | | | |
| V6.0 | Mar. 2016 | Revisión y rectificación | |  |
|  | | | | |
| V7.0 | Nov. 2017 | Revisión |  |  |
| V8.0 | Mar. 2018 | Punto 12.5.1 |  |  |
| V9.0 | Nov. 2018 | Revisión de controles | |  |
| **REVISIÓN Y APROBACIÓN** | | | | |
|  | | | | |
| **COMPAÑÍA** | **NOMBRE** |  | **FECHA** | **FIRMA** |
|  | | | | |
| Sotec | Andrea Vega |  | 25/02/2015 |  |
|  | | | | |
| Sotec | Fernando Ossuna |  | 25/02/2015 |  |
|  | | | | |
| Sotec | David González |  | 18/02/2016 |  |
|  | | | | |
| Sotec | David González, Álvaro Caba | | 01/03/2016 |  |
|  | | | | |
| Sotec | David González, Álvaro Caba | | 23/03/2016 |  |
|  | | | | |
| Sotec | David Gonzalez |  | 17/10/2017 |  |
| Sotec | David Gonzalez |  | 05/03/2018 |  |
| Sotec | David Gonzalez |  | 16/11/2018 |  |