Ficha Procesos Listado Controles y Aplicabilidad

AIRON|B83839571|ISO+ver8.20.762_293

Proceso ES01 DIRECCION Y PLANIFICACION ESTRATEGIA

Detalle Establecimiento de Objetivos. Revisión del Sistema Integrado de Gestión. Gestión de Indicadores para el control de los procesos. Acciones de Mejora. Auditoría Interna. Evaluación de la Satisfacción de Clientes.

Código	Control
No Aplica ☐	
Origen	**Dirección**
Co.Es.01	Supervisión desempeño de Objetivos
Co.Es.02	Supervisión en el cierre de No Conformidades
Co.Es.03	Revisión y tramitación de necesidades y expectativas de PI
Co.Es.04	Supervisión requisitos SG ISO
Co.Es.05	Supervisión actualización normativa
Co.Es.06	Supervisión y recursos CERTIFICACION ISO

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

AIRON|B83839571|ISO+ver8.20.762_293

Proceso SO01 GESTIÓN DE ELEMENTOS DE APOYO

Detalle Elementos de Apoyo al Sistema: Recursos | Personal | Gestión administrativa | Control de la información documentada.

Código	Control
No Aplica ☐	
Origen	**Dirección**
Co.S1.01	Supervisión programas de mantenimiento
Co.S1.02	Control de eficacia de acciones de formación
Co.S1.03	Control y aseguramiento de la distribución documental
Co.S1.04	Supervisión procesos administrativos

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

AIRON|B83839571|ISO+ver8.20.762_293

Proceso SO02 GESTIÓN DE ADMINISTRACIÓN Y COMPRAS

Detalle Descriptivo de información documentada del proceso de control de procesos, productos y servicios suministrados externamente, con el fin de que éstos son conformes a los requisitos.

Código	**Control**
No Aplica	☐
Origen	**Dirección**
Co.S2.01	Inspección en recepción
Co.S2.02	Control documentación de pedidos
Co.S2.03	Seguimiento y supervisión conformidad requisitos de homologación

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

AIRON|B83839571|ISO+ver8.20.762_293

Proceso CL01 GESTIÓN COMERCIAL

Detalle Relación de actividades de comunicación con clientes, preparación de ofertas y tramitación de pedidos.

Código	**Control**
No Aplica ☐	
	Origen **Dirección**
Co.C1.01	Supervisión contratos - pedidos desde dirección de área
Co.C1.02	Control y seguimiento de iniciativas potenciales comerciales

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	01/01/2018	
Responsable SGI Ca&Ma	REVISA	01/01/2018	

Ficha Procesos Listado Controles y Aplicabilidad

AIRON|B83839571|ISO+ver8.20.762_293

Proceso CL02 GESTIÓN DE PRESTACIÓN DE SERVICIOS

Detalle Relación de actividades para la captación y selección de candidatos frente a las diferentes peticiones de los clientes. Control ultimo facturación por el personal en clientes. Gestión administrativa de RRHH.

Código **Control**

No Aplica ☐

Origen **Dirección**

Co.C2.01 Inspección para liberación de servicio - producto: INFORME GESTIÓN INTEGRAL

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

Proceso SO03 GESTIÓN AMBIENTAL

Detalle Revisión de legislación. Requistos Legales. Criterios ambientales. Aspectos. Control Operacional. Medidas de Emergencia.

Código **Control**

No Aplica ☐

Origen	**Dirección**
Co.Am.01	Supervisión cumplimiento control operacional ambiental
Co.Am.02	Supervisión cumplimiento eficacia control emergencias ambientales
Co.Am.03	Supervisión cumplimiento requisitos legales ambientales

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	ALTA EN EL SISTEMA	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

Proceso SO04 GESTIÓN SGSI

Detalle Proceso de Gestión de la Seguridad de la Información.

Código **Control**

No Aplica ☑

Origen **Sistema**

Co.SI.14.2.7. Externalización del desarrollo de software

El desarrollo de software externalizado debe ser supervisado y controlado por la organización.

Co.SI.18.1.5. Regulación de los controles criptográficos

Los controles criptográficos se deben utilizar de acuerdo con todos los contratos, leyes y regulaciones pertinentes.

No Aplica ☐

Origen **Sistema**

Co.SI.05.1.1. Políticas para la seguridad de la información

Se disponen de un conjunto de políticas para la seguridad de la información definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

Co.SI.05.1.2. Revisión de las políticas para la seguridad de la información

Las políticas de seguridad de la información es revisada a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Co.SI.06.1.1. Roles y responsabilidades en seguridad de la información

Todas las responsabilidades en seguridad de la información son definidas y están asignadas.

Co.SI.06.1.2. Segregación de tareas

Las funciones y áreas de responsabilidad están segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

Co.SI.06.1.3. Contacto con las autoridades

Se mantienen los contactos apropiados con las autoridades pertinentes.

Co.SI.06.1.4. Contacto con grupos de interés especial

Son mantenidos los contactos apropiados con grupos de interés especial, foros y asociaciones profesionales especializados en seguridad.

Co.SI.06.1.5. Seguridad de la información en la gestión de proyectos

La seguridad de la información se trata dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

Co.SI.06.2.1. Política de dispositivos móviles

Se adopta una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

Co.SI.06.2.2. Teletrabajo

Se dispone implementada una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

Co.SI.07.1.1. Investigación de antecedentes

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se lleva a cabo de acuerdo con las leyes, normas y códigos éticos que sean de aplicación y es proporcional a las necesidades del negocio, la clasificación de la información a

Co.SI.07.1.2. Términos y condiciones del empleo

Cómo parte de sus obligaciones contractuales, los empleados y contratistas establecen los términos y condiciones de su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

Co.SI.07.2.1. Responsabilidades de gestión

La dirección exigir a los empleados y contratistas, que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos en la organización.

Co.SI.07.2.2. Concienciación, educación y capacitación en seguridad de la información

Todos los empleados de la organización y, cuando corresponda, los contratistas, reciben una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su p

Co.SI.07.2.3. Proceso disciplinario

Se dispone de un proceso disciplinario formal que ha sido comunicado a los empleados, que recoja las acciones a tomar ante aquellos que hayan provocado alguna brecha de seguridad.

Co.SI.07.3.1. Responsabilidades ante la finalización o cambio

Las responsabilidades en seguridad de la información y obligaciones que siguen vigentes después del cambio o finalización del empleo son definidas, comunicadas empleados o contratista y se deben cumplir.

Co.SI.08.1.1. Inventario de activos

Los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario.

Co.SI.08.1.2. Propiedad de los activos

Todos los activos que figuran en el inventario disponen de un propietario.

Co.SI.08.1.3. Uso aceptable de los activos

Se identifican, documentnr e implementan las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

Co.SI.08.1.4. Devolución de activos

Todos los empleados y terceras partes devuelven todos activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

Co.SI.08.2.1. Clasificación de la información

La información es clasificada clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

Co.SI.08.2.2. Etiquetado de la información

Se desarrollan e implantan un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Co.SI.08.2.3. Manipulado de la información

Se desarrollan e implantan un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Co.SI.08.3.1. Gestión de soportes extraíbles

Se disponen implementados procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.

Co.SI.08.3.2. Eliminación de soportes

Los soportes se eliminan de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales.

Co.SI.08.3.3. Soportes físicos en tránsito

Durante el transporte fuera de los límites físicos de la organización, los soportes que contengan información estan protegidos contra accesos no autorizados, usos indebidos o deterioro.

Co.SI.09.1.1. Política de control de acceso

Se establecen, documentan y revisan una política de de acceso basada en los requisitos de negocio y de seguridad de la información.

Co.SI.09.1.2. Acceso a las redes y a los servicios de red

Únicamente se proporcionan a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

Ficha Procesos Listado Controles y Aplicabilidad

Co.SI.09.2.1. Registro y baja de usuario

Se dispone implantado un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de los derechos de acceso.

Co.SI.09.2.2. Provisión de acceso de usuario

Se dispone implantado un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

Co.SI.09.2.3. Gestión de privilegios de acceso

La asignación y el uso de privilegios de acceso es restringida y controlada.

Co.SI.09.2.4. Gestión de la información secreta de autenticación de los usuarios

La asignación de la información secreta de autenticación es controlada a través de un proceso formal de gestión.

Co.SI.09.2.5. Revisión de los derechos de acceso de usuario

Los propietarios de los activos revisan los derechos de acceso de usuario a intervalos regulares.

Co.SI.09.2.6. Retirada o reasignación de los derechos de acceso

Los derechos de acceso de todos los empleados y terceras partes, a la información y a los recursos de tratamiento de la información son retirados a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio.

Co.SI.09.3.1. Uso de la información secreta de autenticación

Se requiere a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

Co.SI.09.4.1. Restricción del acceso a la información

Se restringe el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de de acceso definida.

Co.SI.09.4.2. Procedimientos seguros de inicio de sesión

Cuando así se requiera en la política de de acceso, el acceso a los sistemas y a las aplicaciones so controla por medio de un procedimiento seguro de inicio de sesión.

Co.SI.09.4.3. Sistema de gestión de contraseñas

Los sistemas para la gestión de contraseñas son interactivos y establecen contraseñas seguras y robustas.

Co.SI.09.4.4. Uso de utilidades con privilegios del sistema

Se restringe y controlan rigurosamente el uso de utilidades que puedan ser capaces de invalidar los controles del sistema y de la aplicación.

Co.SI.09.4.5. Control de acceso al código fuente de los programas

Se restringe el acceso al código fuente de los programas.

Co.SI.10.1.1. Política de uso de los controles criptográficos

Se desarrolla e implementa una política sobre el uso de los controles criptográficos para proteger la información.

Co.SI.10.1.2. Gestión de claves

Se desarrolla e implementa una política de sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

Co.SI.11.1.1. Perímetro de seguridad física

Se utilizan perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.

Co.SI.11.1.2. Controles físicos de entrada

Las áreas seguras estan protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

Co.SI.11.1.3. Seguridad de oficinas, despachos y recursos

Para las oficinas, despachos y recursos, se diponen diseños y aplica la seguridad física.

Co.SI.11.1.4. Protección contra las amenazas externas y ambientales

Se diponen diseños y aplica una protección física contra desastres naturales, ataques provocados por el hombre o accidentes.

Co.SI.11.1.5. El trabajo en áreas seguras

Se dipone diseño e implementados procedimientos para trabajar en las áreas seguras.

Co.SI.11.1.6. Áreas de carga y descarga

Se controlan los puntos de acceso tales como las áreas de carga y descarga y otros puntos, donde pueda acceder personal no autorizado a las instalaciones, y si es posible, aislar dichos puntos de los recursos de tratamiento de la información para evitar a

Co.SI.11.2.1. Emplazamiento y protección de equipos

Los equipos se situan o protegen de forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales así como las oportunidades de que se produzcan accesos no autorizados.

Co.SI.11.2.2. Instalaciones de suministro

Los equipos están protegidos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.

Co.SI.11.2.3. Seguridad del cableado

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información están protegidos frente a interceptaciones, interferencias o daños.

Co.SI.11.2.4. Mantenimiento de los equipos

Los equipos reciben un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.

Co.SI.11.2.5. Retirada de materiales propiedad de la empresa

Sin autorización previa, los equipos, la información o el software no se sacan de las instalaciones.

Co.SI.11.2.6. Seguridad de los equipos fuera de las instalaciones

Se aplican medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.

Co.SI.11.2.7. Reutilización o eliminación segura de equipos

Todos los soportes de almacenamiento son comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos.

Co.SI.11.2.8. Equipo de usuario desatendido

Los usuarios se aseguran que el equipo desatendido tiene la protección adecuada.

Co.SI.11.2.9. Política de puesto de trabajo despejado y pantalla limpia

Se dispone adoptado una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y una política de pantalla limpia para los recursos de tratamiento de la información.

Co.SI.12.1.1. Documentación de procedimientos de los operación

Se dispone documentado y se mantiene procedimientos de operación y se ponen a disposición de todos los usuarios que los necesiten.

Co.SI.12.1.2. Gestión de cambios

Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información son controlados.

Co.SI.12.1.3. Gestión de capacidades

Se supervisan y ajusta la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

Co.SI.12.1.4. Separación de los recursos de desarrollo, prueba y operación

Se diponen separados los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

Co.SI.12.2.1. Controles contra el código malicioso

Se disponen implementados los controles de detección, prevención y recuperación que sirvan como protección contra el código malicioso, así como procedimientos adecuados de concienciación al usuario.

Co.SI.12.3.1. Copias de seguridad de la información

Se realizan copias de seguridad de la información, del software y del sistema y se deben verificar periódicamente de acuerdo a la política de copias de seguridad acordada.

Co.SI.12.4.1. Registro de eventos

Se registran, protegen y revisan periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Co.SI.12.4.2. Protección de la información de registro

Los dispositivos de registro y la información del registro estan protegidos contra manipulaciones indebidas y accesos no autorizados.

Co.SI.12.4.3. Registros de administración y operación

Se registran, protegen y revisan regularmente las actividades del administrador del sistema y del operador del sistema.

Co.SI.12.4.4. Sincronización del reloj

Los relojes de todos los sistemas de tratamiento de información dentro de una organización o de un dominio de seguridad, estan sincronizados con una única fuente precisa y acordada de tiempo.

Co.SI.12.5.1. Instalación del software en explotación

Se disponen implementados procedimientos para controlar la instalación del software en explotación.

Co.SI.12.6.1. Gestión de las vulnerabilidades técnicas

Se obtiene información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

Co.SI.12.6.2. Restricción en la instalación de software

Se disponen establecidas y aplican reglas que rijan la instalación de software por parte de los usuarios.

Co.SI.12.7.1. Controles de auditoría de sistemas de información

Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos son cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.

Co.SI.13.1.1. Controles de red

Las redes son gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

Co.SI.13.1.2. Seguridad de los servicios de red

Se identifican los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se incluyen en acuerdos de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontr

Co.SI.13.1.3. Segregación en redes

Los grupos de servicios de información, los usuarios y los sistemas de información estan segregados en redes distintas.

Co.SI.13.2.1. Políticas y procedimientos de intercambio de información

Se establecen políticas, procedimientos y controles formales que protegen el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

Co.SI.13.2.2. Acuerdos de intercambio de información

Se establecen acuerdos para el intercambio seguro de información del negocio y software entre la organización y terceros.

Co.SI.13.2.3. Mensajería electrónica

La información que sea objeto de mensajería electrónica está adecuadamente protegida.

Co.SI.13.2.4. Acuerdos de confidencialidad o no revelación

Se identifican, documentan y revisan regularmente los requisitos de los acuerdos de confidencialidad o no revelación

Co.SI.14.1.1. Análisis de requisitos y especificaciones de seguridad de la información

Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

Co.SI.14.1.2. Asegurar los servicios de aplicaciones en redes públicas

La información involucrada en aplicaciones que pasan a través de redes públicas es protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.

Co.SI.14.1.3. Protección de las transacciones de servicios de aplicaciones

La información involucrada en las transacciones de servicios de aplicaciones es protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autori

Co.SI.14.2.1. Política de desarrollo seguro

Se establecen y aplican reglas dentro de la organización para el desarrollo de aplicaciones y sistemas.

Co.SI.14.2.2. Procedimiento de control de cambios en sistemas

La implantación de cambios a lo largo del ciclo de vida del desarrollo debe controlarse mediante el uso de procedimientos formales de cambios.

Co.SI.14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Cuando se modifiquen los sistemas operativos, las aplicaciones de negocio críticas son revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización.

Co.SI.14.2.4. Restricciones a los cambios en los paquetes de software

Se desaconsejan las modificaciones en los paquetes de software, limitándose a los cambios necesarios, y todos los cambios son objeto de un riguroso control.

Co.SI.14.2.5. Principios de ingeniería de sistemas seguros

Principios de ingeniería de sistemas seguros se establecen, documentan, mantiene y aplican a todos los esfuerzos de implementación de sistemas de información.

Co.SI.14.2.6. Entorno de desarrollo seguro

La organización establece y protege adecuadamente los entornos de desarrollo seguro para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo del sistema.

Co.SI.14.2.8. Pruebas funcionales de seguridad de sistemas

Se llevan a cabo pruebas de la seguridad funcional durante el desarrollo.

Co.SI.14.2.9. Pruebas de aceptación de sistemas

Se establecen programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

Co.SI.14.3.1. Protección de los datos de prueba

Los datos de prueba se seleccionan con cuidado y son protegidos y controlados.

Co.SI.15.1.1. Política de seguridad de la información en las relaciones con los proveedores

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización son acordados con el proveedor y quedan documentados.

Co.SI.15.1.2. Requisitos de seguridad en contratos con terceros

Todos los requisitos relacionados con la seguridad de la información son establecidos y se acuerdan con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.

Co.SI.15.1.3. Cadena de suministro de tecnología de la información y de las comunicaciones

Los acuerdos con proveedores incluyen requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

Co.SI.15.2.1. Control y revisión de la provisión de servicios del proveedor

La organización controla, revisa y audita regularmente la provisión de servicios del proveedor.

Co.SI.15.2.2. Gestión de cambios en la provisión del servicio del proveedor

Se gestionan los cambios en la provisión del servicio, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y es de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de negocio afec

Co.SI.16.1.1. Responsabilidades y procedimientos

Se establecen las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

Co.SI.16.1.2. Notificación de los eventos de seguridad de la información

Los eventos de seguridad de la información se notifican por los canales de gestión adecuados lo antes posible.

Co.SI.16.1.3. Notificación de puntos débiles de la seguridad

Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deben ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.

Co.SI.16.1.4. Evaluación y decisión sobre los eventos de seguridad de información

Los eventos de seguridad de la información son evaluados y se decide si se clasifican como incidentes de seguridad de la información.

Co.SI.16.1.5. Respuesta a incidentes de seguridad de la información

Los incidentes de seguridad de la información son respondidos de acuerdo con los procedimientos documentados.

Co.SI.16.1.6. Aprendizaje de los incidentes de seguridad de la información

El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de información se utilizan para reducir la probabilidad o el impacto de los incidentes en el futuro.

Co.SI.16.1.7. Recopilación de evidencias

La organización define y aplica procedimientos para la identificación recogida, adquisición y preservación de información que puede servir de evidencia.

Co.SI.17.1.1. Planificación de la continuidad de la seguridad de la información

La organización determina sus necesidades de seguridad de la información y de continuidad para la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

Co.SI.17.1.2. Implementar la continuidad de la seguridad de la información

La organización establece, documenta, implementa y mantiene procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Co.SI.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La organización comprueba los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

Co.SI.17.2.1. Disponibilidad de los recursos de tratamiento de la información

Los recursos de tratamiento de la información son implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

Co.SI.18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, son definidos de forma explícita, documentarse y mantenerse actualizados para cada sistema de informac

Co.SI.18.1.2. Derechos de propiedad intelectual (DPI)

Se implementan procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de prod

Co.SI.18.1.3. Protección de los registros de la organización

Los registros estan protegidos contra la pérdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

Co.SI.18.1.4. Protección y privacidad de la información de carácter personal

Se garantiza la protección y la privacidad de los datos, según se requiera en la legislación y la reglamentación aplicables.

Co.SI.18.2.1. Revisión independiente de la seguridad de la información

El enfoque de la organización para la gestión de seguridad de la información y su implantación (es decir, objetivos de , controleses, políticas, procesos y procedimientos para la seguridad de la información), se someten a una revisión independiente a int

Co.SI.18.2.2. Cumplimiento de las políticas y normas de seguridad

Los directivos aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable

Co.SI.18.2.3. Comprobación del cumplimiento técnico

Se comprueba periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información.

Ficha Procesos Listado Controles y Aplicabilidad

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	Primera edicion. Alta en el Sistema.	DECLARACIÓN DE APLICABILIDAD PRIMERA EDICION (Referencia Enero'1)

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	

Ficha Procesos Listado Controles y Aplicabilidad

Proceso SO05 GESTIÓN DE SERVICIO IT (SGS)

Detalle Detalle del proceso de la Gestión de los Servicios IT

Código	Control	Origen
Co.SMS.01	Control cumplimiento SLA's SERVICIOS INTERNOS	
Co.SMS.02	Control cumplimiento SLA's SERVICIOS EXTERNOS	
Co.SMS.03	Control cumplimiento SLA's SERVICIOS EXTERNALIZADOS	
Co.SMS.04	Control disposición de acuerdor de servicio	
Co.SMS.05	Publicación de informes de servicios y revisión de cumplimiento RQ	

No Aplica ☐

Historial de Revisión

Revisión Nº	Detalle	Desarrollo
1	Primera edicion. Alta en el Sistema.	

Interviniente	Tipo	Fecha	Detalle
DIRECTOR GENERAL	APRUEBA	30/01/2019	
Responsable SGI Ca&Ma	REVISA	30/01/2019	