4.1. DOMINIO 5: Política de Seguridad

Dominio	**5.**	**POLÍTICA DE SEGURIDAD**
Categoría	**5.1.**	**Política de seguridad de la información**
Control	**5.1.1.**	**Documento de política de seguridad de la información.**
Objetivo	Aprobar, publicar y comunicar, por parte de gerencia a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información	
Procedimientos Específicos	P1	**Definición, objetivos globales, alcance e importancia** Verificar que exista una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
	P2	**Apoyo de gerencia** Verificar si se ha establecido el objetivo de la gerencia como soporte de los principios y objetivos de la seguridad de la información.
	P3	**Objetivos de control y mandos.** Comprobar si se definió un marco para colocar los objetivos de control y mandos, incluyendo la estructura de riesgo y gestión del riesgo.
	P4	**Políticas, principios, normas y requisitos** Constatar que se definen las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo: conformidad con los requisitos legislativos y contractuales, requisitos de formación en seguridad, gestión de la continuidad del negocio, consecuencias de las violaciones de la política de seguridad.
	P5	**Responsabilidades y comunicación de incidencias** Verificar la definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad.
	P6	**Referencias de documentación** Constatar que se hayan referenciado documentación que pueda sustentar la política, por ejemplo: políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.
Documentos por revisar	D1	Políticas, principios, normas y requisitos en seguridad de la información
	D2	Documento de trazabilidad de funciones.
	D3	Procedimientos de comunicación de incidencias.

Dominio	**5.**	**POLÍTICA DE SEGURIDAD**
Categoría	**5.1.**	**Política de seguridad de la información**
Control	**5.1.2.**	**Revisión y evaluación**
Objetivo	Revisar la política de seguridad en intervalos planificados o si cambios significantes ocurren con el fin de asegurar su uso continuo.	
Procedimientos Específicos	P1	**Propietario de la política** Comprobar si la política tiene un propietario que sea responsable del desarrollo, revisión y evaluación de la política de seguridad.
	P2	**Revisión de la política** Verificar la existencia de procedimientos definidos de la gestión de revisión, incluyendo un calendario o periodo de revisión. Incluye aprobación gerencial.
Documentos por revisar	D1	Políticas, principios, normas y requisitos en seguridad de la información
	D2	Procedimientos para la gestión de la revisión.

4.2. DOMINIO 6: Aspectos Organizativos para la Seguridad

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.1.**	**Comité de gestión de seguridad de la información**
Objetivo	Apoyar activamente en la seguridad dentro de la organización a través de direcciones claras demostrando compromiso, asignaciones explícitas y reconocimiento de las responsabilidades de la seguridad de información	
Procedimientos Específicos	P1	**Integrar metas de Seguridad de Información con las exigencias organizacionales.** Verificar que el comité asegure que las metas de la seguridad de información sean identificadas, relacionarlas con las exigencias organizacionales y que sean integradas en procesos relevantes.
	P2	**Política de Seguridad de Información** Comprobar que el comité haya formulado, revisado y aprobado la política de seguridad de información
	P3	**Implementación de la política de información.** Verificar que el comité revisó la efectividad en la implementación de la política de información.
	P4	**Dirección y gestión** Constatar que el comité provee direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad
	P5	**Recursos para seguridad de información** Verificar que el comité proveyó los recursos necesarios para la seguridad de la información.
	P6	**Roles y responsabilidades** Comprobar que el comité aprobó asignaciones de roles específicos y responsabilidades para seguridad de información a través de la organización.
	P7	**Planes y programas de concientización** Constatar que el comité inicia planes y programa para mantener la conciencia en seguridad de información.
	P8	**Implementación de controles** Verificar que el comité haya asegurado que la implementación de los controles de la seguridad de información es coordinada a través de la organización
Documentos a revisar	D1	Estructura, roles, funciones y responsabilidades del comité de gestión de seguridad de la información
	D2	Política de Seguridad de Información
	D3	Documento de implementación de la Política de Seguridad de Información
	D4	Documento de recursos designados para seguridad de información
	D5	Portafolio de programas de concientización
	D6	Documento de implementación de controles de Seguridad de Información

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.2.**	**Coordinación de la seguridad de la información**
Objetivo	Coordinar la información de las actividades de seguridad mediante representantes de las diferentes partes de la organización con roles relevantes y funciones de trabajo.	
Procedimientos Específicos	P1	**Ejecutar actividades de seguridad en cumplimiento con política de seguridad.** Verificar el aseguramiento que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad.
	P2	**Manejo de no cumplimientos** Comprobar que se identifique como manejar los no cumplimientos
	P3	**Aprobar metodologías y procesos para seguridad de información.** Verificar que se apruebe las metodologías y procesos para seguridad de información, como por ejemplo la evaluación del riesgo y la clasificación de información.
	P4	**Cambios significativos de amenazas y exposición de información** Constatar que se identifique los cambios significativos en las amenazas y exposición de información.
	P5	**Adecuación e implantación de los controles de seguridad de información.** Constatar que se evalúe la adecuación y coordine la implantación de los controles de seguridad de la información.
	P6	**Educar y concientizar en seguridad de información** Comprobar que se promocione efectivamente la educación, entrenamiento y concientización en seguridad de información, a través de la organización.
	P7	**Monitoreo y revisión de incidentes** Acreditar que se evalúa la información de seguridad recibida de monitorear, revisa los incidentes de seguridad de información y recomienda acciones apropiadas en respuesta para identificar incidentes de seguridad de información.
Documentos por revisar	D1	Estructura organizacional de la empresa
	D2	Documento de implementación de la Política de Seguridad de Información

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.3.**	**Asignación de responsabilidades sobre seguridad de la información**
Objetivo	Definir claramente las responsabilidades	
Procedimientos Específicos	P1	**Identificar activos y procesos de seguridad** Verificar que se identifiquen claramente los activos y los procesos de seguridad acosiados con cada sistema específico.
	P2	**Responsables de cada activo o proceso de seguridad** Constatar que se nombren responsables de cada activo o proceso de seguridad y documentar los detalles de estas responsabilidades
	P3	**Niveles de autorización** Verificar que se definan y documenten claramente los niveles de autorización
Documentos por revisar	D1	Documento de trazabilidad de responsabilidades.
	D2	Documento de niveles de autorización.

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.4.**	**Proceso de autorización de recursos para el tratamiento de la información**
Objetivo	Establecer un proceso de autorización para la gestión de cada nuevo recurso de tratamiento de la información	
Procedimientos Específicos	P1	**Aprobación de nuevos medios** Verificar que los nuevos medios tengan aprobación adecuada de la gerencia de usuario, autorizando su propósito y uso. También debería obtenerse la aprobación del directivo responsable del mantenimiento del entorno de seguridad del sistema de información local, asegurando que cumple con todas las políticas y requisitos de seguridad correspondientes.
	P2	**Compatibilidad** Comprobar que el hardware y software son compatibles con los demás dispositivos del sistema
	P3	**Autorizar y evaluar uso de medios informáticos personales** Verificar la autorización y evaluación del uso de medios informáticos personales, como laptops o aparatos móviles, para el tratamiento de la información de la organización así como los controles necesarios, ya que introducen nuevas vulnerabilidades
Documentos por revisar	D1	Documento de nuevos medios con sus respectivas aprobaciones
	D2	Registro de medios informáticos personales.
	D3	Autorizaciones de los medios informáticos personales
	D4	Políticas para medios informáticos personales.

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.5.**	**Acuerdos de confidencialidad**
Objetivo	Identificar y revisar regularmente los requerimientos de confidencialidad o acuerdos de no divulgación que reflejen necesidades de la organización para la protección de información.	
Procedimientos Específicos	P1	**Información a ser protegida** Verificar la existencia de una definición de la información a ser protegida.
	P2	**Duración esperada del acuerdo** Comprobar que exista una duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda ser mantenida indefinidamente.
	P3	**Acciones cuando un acuerdo es finalizado** Comprobar que existan acciones requeridas cuando un acuerdo es finalizado
	P4	**Responsabilidades y acciones** Constatar la existencia de responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información.
	P5	**Protección de la información confidencialidad** Verificar que se haya especificado la propiedad de la información, secretos del comercio y de la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.
	P6	**Permisos** Verificar los permisos de utilizar información confidencial y los derechos del signatario para usar la información.
	P7	**Auditoria y monitoreo** Constatar que se realicen auditorias y monitoreos de las actividades que impliquen información confidencial.
	P8	**Cesión del acuerdo** Verificar que existan términos para que la información sea retornada o destruida en la cesión del acuerdo.
	P9	**Abertura del acuerdo** Verificar que se tengan acciones previstas que se tomará en caso de abertura del acuerdo.
Documentos por revisar	D1	Documentos de acuerdos de confidencialidad
	D2	Requerimientos de seguridad de la organización
	D3	Reportes de actualización de los acuerdos de confidencialidad

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.6.**	**Contacto con autoridades.**
Objetivo	Mantener los contactos apropiados con autoridades relevantes.	
Procedimientos Específicos	P1	**Procedimientos de contacto** Constatar que la organización tiene procedimientos instalados que especifican cuando y por qué autoridades deben ser contactadas y como los incidentes identificados en la seguridad de información deben ser reportados de una manera oportuna si se sospecha que las leyes han sido rotas.
	P2	**Ataque desde Internet** Constatar que, bajo ataque desde el Internet, se tiene un canal de comunicación con terceros (como por ejemplo: el proveedor del servicio de Internet o el operador de telecomunicaciones).
Documentos por revisar	D1	Documento de canales de comunicación.
	D2	Requerimientos de seguridad de la organización

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.7.**	**Contacto con grupos de interés especial**
Objetivo	Mantener contactos apropiados con grupos de interés especial u otros especialistas en foros de seguridad y asociaciones profesionales.	
Procedimientos Específicos	P1	**Membresía en grupos de interés especial** Constatar que se tengan membresías de grupos de interés especial profesionales
Documentos por revisar	D1	Lista de membresías en grupos de interés.
	D2	Documentación de los conocimientos implantados en la organización
	D3	Reportes de actualización de los acuerdos de confidencialidad

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.1.**	**Organización interna**
Control	**6.1.8.**	**Revisión independiente de la seguridad de la información**
Objetivo	Revisar de manera independiente en tiempos planificados o cuando ocurran cambios significativos el alcance de la organización para gestionar la Seguridad de la Información y su implementación.	
Procedimientos Específicos	P1	**Revisión independiente** Constatar que la revisión independiente es iniciada por la gerencia y que incluya oportunidades de evaluación para mejorar y la necesidad de cambios para el acercamiento a la seguridad, incluyendo la política y los objetivos de control.
	P2	**Ejecutores de la revisión** Verificar que la revisión independiente sea llevada a cabo por individuos independientes del área bajo revisión.
	P3	**Habilidades y experiencia de los ejecutores** Verificar que los individuos que lleven a cabo las revisiones tengan las habilidades y experiencia apropiada.
	P4	**Resultados de la revisión** Constatar que se registre y reporte a gerencia que inició la revisión.
	P5	**Mantenimiento de los resultados de la revisión** Verificar que los resultados obtenidos de las revisiones independientes estén mantenidos por la organización
	P6	**Consideraciones correctivas.** Constatar que si la revisión independiente identifica que el alcance de la organización o la implementación de la gestión de seguridad de información es inadecuada o no complaciente con la dirección de seguridad de información establecida en la política, la gerencia considere acciones correctivas
Documentos por revisar	D1	Resultados de revisiones independientes
	D2	Documentos de pase a ejecución de las revisiones independientes (donde se especifique qué gerencia está iniciándola)
	D3	Documentos de información del equipo de individuos ejecutores de la revisión.

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.2.**	**Seguridad en los accesos de terceras partes**
Control	**6.2.1.**	**Identificación de riesgos por el acceso de terceros**
Objetivo	Identificar e implementar controles antes de conceder a terceros acceso a la información de la organización y las instalaciones que las procesa.	
Procedimientos Específicos	P1	**Identificación de riesgos relacionados.** Constatar que se identificaron los riesgos relacionados con el acceso a terceros considerando: a) Las instalaciones del procesamiento de la información a la que terceros requieren acceso b) El tipo de acceso que terceros tendrán a la información y a las instalaciones del procesamiento de infamación: 1) acceso físico, por ejemplo oficinas o salas de ordenadores 2) acceso lógico, por ejemplo la base de datos de la organización o sistemas de información 3) conectividad de red entre la organización y terceros, por ejemplo la conexión permanente o acceso remoto 4) si el acceso esta ocurriendo en el sitio o fuera de el c) el valor y la sensibilidad de la información implicada, y es critico para operaciones de negocios d) los controles necesarios para proteger la información que no debe ser accesible a terceros e) el personero externo implicado en maniobrar la información de la organización f) como la organización o el personero autorizado para tener acceso puede ser identificado, la autorización verificada y que tan seguido necesita ser reconfirmada g) los diferentes significados y controles empleados por terceros cuando guarde, procese, comunique, comparta e intercambia información h) el impacto del acceso no disponible a terceros cuando sea requerido, y de terceros ingresando o recibiendo información inexacta o engañosa i) prácticas y procedimientos para lidiar con incidentes y daños potenciales en la seguridad de información, y los términos y condiciones para continuar con el acceso a terceros en el caso de un incidente en la seguridad de información j) requisitos legales y regulatorios u otras obligaciones contractuales relevantes a terceros que deben ser tomadas en cuenta. k) como los intereses de las partes interesadas pueden ser afectados por los acuerdos.
	P2	**Provisión de acceso** Constatar que el acceso a terceras personas a la información de la organización no sea provista hasta que se haya implementado los controles apropiados y que éstos sean factibles

	P3	**Comunicación de las obligaciones del tercero** Constatar que las terceras personas estén enteradas de sus obligaciones y que acepten las responsabilidades que implica acceder, procesar, comunicar o manejar la información de la organización y las instalaciones del procesamiento de información.
Documentos a revisar	D1	Documento de riesgos.
	D2	Documentos de accesos a terceros
	D3	Documentos de obligaciones y responsabilidades de terceros por el acceso provisto.

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.2.**	**Seguridad en los accesos de terceras partes**
Control	**6.2.2.**	**Requisitos de seguridad cuando sea trata con clientes**
Objetivo	Todos los requisitos identificados de seguridad deben ser anexados antes de dar a los clientes acceso a la información o a los activos de la organización.	
Procedimientos Específicos	P1	Verificar que los siguientes términos son considerados para ser anexados a la seguridad antes de dar a los clientes acceso a los activos de seguridad (dependiendo del tipo y la extensión del acceso dado, no todos aplican): a) protección de activos, incluyendo: 1) procedimientos para proteger los activos de la organización, incluida la información y el software. 2) procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos. 3) medidas de integridad. 4) restricciones en la copia o divulgación de la información. b) la descripción del servicio o producto disponible; c) las diferentes razones, requerimientos y beneficios para el acceso del cliente. d) acuerdos sobre control de accesos, incluyendo: 1) los métodos de acceso permitidos, así como el control y uso de identificadores únicos, como número de identificación ID y contraseñas. 2) el procedimiento de autorización del acceso y privilegios a los usuarios. 3) una declaración de que todo acceso que no esta explícitamente autorizado es prohibido. 4) un proceso para revocar el derecho de acceso o interrumpir la conexión entre sistemas. e) arreglos para reportar, notificar e investigar inexactitudes de información (como detalles personales), incidentes y aberturas en la seguridad de información. f) una descripción de cada servicio a ser disponible. g) el nivel de servicio. h) el derecho para controlar y revocar cualquier actividad relacionado con los activos de la organización. i) las respectivas responsabilidades de la organización y de los clientes; j) las responsabilidades en materia de legislación por ejemplo sobre protección de datos personales, teniendo especialmente en cuenta los diferentes sistemas legales nacionales si el contrato implica la cooperación con organizaciones de otros países (véase también el inciso 15.1). k) los derechos de propiedad intelectual, protección contra copias (véase el inciso 15.1.2.) y protección en tareas de colaboración (véase también el inciso 6.1.5).
Documentos a revisar	D1	Documento de requisitos de seguridad de la organización
	D2	Documentos de procedimientos de control de accesos

Dominio	**6**	**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**
Categoría	**6.2.**	**Seguridad en los accesos de terceras partes**
Control	**6.2.3.**	**Requisitos de seguridad cuando sea trata con clientes**
Objetivo	Los acuerdos con terceras partes que impliquen acceso, proceso comunicación o gestión de la información de la organización deben cubrir los requisitos de seguridad relevantes	
Procedimientos Específicos	P1	**Acuerdo con terceras partes** Verificar que el acuerdo asegure que no existe desentendimiento entre la organización y las terceras partes. Que la organización se satisfaga en cuento a la indemnidad del tercero. Considerar los siguientes términos: a) la política de información de seguridad b) los controles que aseguren la protección del activo, incluyendo: 1) procedimientos para proteger los activos organizacionales, incluyendo información, software y hardware. 2) controles cualquiera de protección física requerida y mecanismos. 3) controles para asegurar la protección contra software malicioso. 4) procedimientos para determinar si es que se compromete el activo, como pérdida o modificación de la información, software y hardware, ha ocurrido. 5) controles que aseguran el retorno o la destrucción de información y activos al final de o de un tiempo acordado durante el acuerdo. 6) confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante (véase el inciso 2.1.5) de los activos 7) restricciones para copiar y divulgar información y el uso de acuerdos de confidencialidad. c) capacitación en los métodos, procedimientos y seguridad para usuario y administrador. d) asegurar el conocimiento del usuario para temas y responsabilidades de la seguridad de información. e) disposición para transferir personal, cuando sea apropiado. f) responsabilidades con respecto a la instalación y el mantenimiento del hardware y software. g) una clara estructura y formatos de reportes h) un claro y especificado proceso de cambio de gestión. i) política de control de acceso, cubriendo: 1) las diferentes razones, requerimientos y beneficios que hacen el acceso por terceros necesario. 2) métodos permitidos de acceso y el control y uso de identificadores únicos como ID de usuario y contraseñas. 3) un proceso autorizado para acceso de usuarios y los privilegios.

		4) un requerimiento para mantener una lista de individuos autorizados a usar el servicio que ha sido disponible y cual son sus derechos y privilegios respecto a su uso. 5) una declaración de que todos los accesos que no son explícitamente autorizados son prohibidos; j) arreglos para reportar, notificar e investigar incidentes de la seguridad de información y aperturas de seguridad, como violaciones de los requerimientos establecidos en el acuerdo. K) una descripción del producto o servicio ha ser provisto y una descripción de la información ha ser disponible de acuerdo con su clasificación de seguridad (véase el inciso 7.2.1). l) el objetivo de nivel de servicio y los niveles de no aceptación. m) la definición del criterio de comprobación del funcionamiento, su control y su reporte. n) el derecho de controlar y revocar cualquier actividad relacionada con los activos de la organización. o) el derecho para auditar responsabilidades definidas en el acuerdo, para que dichas auditorias sean llevadas a cabo por terceros y para enumerar los derechos estatutarios de los auditores; p) el establecimiento de un proceso de escalamiento para resolver problemas. q) requisitos continuos de servicio, incluyendo medidas para la disponibilidad y la confiabilidad, en concordancia con las prioridades de negocio de la organización. r) las respectivas responsabilidades de las partes del acuerdo. s) responsabilidades con respecto a temas legales y como se asegura que los requerimientos legales sean conocidos, como por ejemplo la legislación de protección de datos, considerar especialmente diversos sistemas legislativos nacionales si el acuerdo implica la cooperación con organizaciones de otros países (véase el inciso 6.1.5). t) derechos de propiedad intelectual y de asignación de copyright y protección de cualquier otro trabajo de colaboración (véase también 6.1.5). u) implicancias entre los sub-contratantes y terceros, y los controles de seguridad que estos sub-contratantes necesitan implementar. v) condiciones para la renegociación/terminación de los acuerdos: 1) un plan de contingencia debe llevarse a cabo en caso de que cualquiera de las partes desee cortar relaciones antes del término de los acuerdos. 2) renegociación de los acuerdos si los requisitos de seguridad de la organización cambian. 3) documentación actual de la lista de activos, licencias, acuerdos o derechos relacionados con ellos.
	P2	**Incapacidad por terceras partes de suministrar servicios** Verificar la existencia de procedimientos para el proceso continuo en el acuerdo en el caso de que las terceras partes sean incapaces de suministrar sus servicios.
Documentos a	D1	Documento de riesgos

revisar	D2	Documento de requisitos de seguridad
	D3	Plan de gestión de seguridad
	D4	Documento de acuerdos con terceros

4.3. DOMINIO 7: Clasificación y control de Activo

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**
Categoría	**7.1.**	**Responsabilidad sobre los activos**
Control	**7.1.1.**	**Inventario de activos**
Objetivo	Identificar todos los activos elaborando y manteniendo un inventario de todos los activos importantes.	
Procedimientos Específicos	P1	**Identificación de activos** Constatar que la organización identificó todos los activos y la documentación de importancia de ellos. Debe incluir toda la información necesaria con el fin de recuperarse de un desastre, incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencia y el valor dentro del negocio.
	P2	**Clasificación de activos** Verificar que los propietarios y la clasificación de la información debe ser aceptada y documentada para cada uno de los activos.
Documentos por revisar	D1	Documento de Identificación de activos
	D2	Inventario de activos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**
Categoría	**7.1.**	**Responsabilidad sobre los activos**
Control	**7.1.2.**	**Propiedad de los activos**
Objetivo	Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización.	
Procedimientos Específicos	P1	**Responsabilidad de propietarios de activos** Verificar que los propietarios sean responsables por: a) asegurar que la información y los activos asociados con las instalaciones de procesamiento de información son apropiadamente clasificadas. b) definiendo y revisando periódicamente las restricciones de acceso y las clasificaciones, tomando en cuenta políticas de control aplicables.
	P2	**Asignación de propiedad.** Verificar que la propiedad haya sido asignada a: a) proceso de negocios b) un conjunto definido de actividades c) una paliación, o d) un conjunto definido de datos.
Documentos por revisar	D1	Documento de responsabilidades sobre activos.
	D2	Documento de asignación de propiedad sobre activos.

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**
Categoría	**7.1.**	**Responsabilidad sobre los activos**
Control	**7.1.3.**	**Uso adecuado de los activos**
Objetivo	Identificar, documentar e implementar las reglas para un uso aceptable de la información y de los activos asociados con las instalaciones del procesamiento de la información.	
Procedimientos Específicos	P1	**Reglas para empleados, contratistas y terceras partes** Comprobar que los empleados, contratistas y terceras partes sigan: a) las reglas para correo electrónico y usos de Internet (véase el inciso 10.8). b) las guías para el uso de aparatos móviles, especialmente para el uso fuera de las premisas de la organización (véase el inciso 11.7.1).
	P2	**Provisión de reglas específicas** Verificar que se haya implementado medidas tecinas y organizacionales apropiadas para proteger la información personal
Documentos por revisar	D1	Guías provistas por la gerencia sobre el uso adecuado de los activos

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**
Categoría	**7.2.**	**Clasificación de la información**
Control	**7.2.1.**	**Guías de clasificación**
Objetivo	Clasificar la información en función de su valor, requisitos legales, sensibilidad y criticidad para la organización	
Procedimientos Específicos	P1	**Impactos de compartir o restringir información** Verificar que se analizó los impactos en la organización asociado a la necesidad de compartir o restringir la información de la organización.
	P2	**Reclasificación a través del tiempo** Constatar que se tiene convenciones para la reclasificación a través del tiempo, en concordancia con algunas políticas de control predeterminadas (véase 11.1.1.)
	P3	**Responsabilidad del propietario del activo** Constatar que el propietario del activo define la clasificación de éste, lo revisa periódicamente y que asegure que está actualizado y en un nivel apropiado.
Documentos por revisar	D1	Documento de Clasificación de activos
	D2	Políticas de control de activos.
	D3	Documento de análisis de impacto.

Dominio	**7.**	**CLASIFICACIÓN Y CONTROL DE ACTIVOS**
Categoría	**7.2.**	**Clasificación de la información**
Control	**7.2.2.**	**Marcado y tratamiento de la información**
Objetivo	Definir un conjunto adecuado de procedimientos para marcar y tratar la información de acuerdo con el esquema de clasificación adoptado por la organización	
Procedimientos Específicos	P1	**Alcance de los procedimientos de marcado de la información** Corroborar que los procedimientos para el marcado de la información cubra los activos en formato físico y electrónico.
	P2	**Marcado en la salida de sistemas de información.** Verificar que la salida procedente de los sistemas que traten información clasificada como sensible o crítica lleven una etiqueta de clasificación adecuada (en la salida) que refleje la clasificación de acuerdo con las reglas establecidas en 7.2.1.
	P3	**Definición de procedimientos** Comprobar que para cada nivel de clasificación, se han definido los procedimientos de manipulación incluyendo el procesamiento seguro, copia, almacenamiento, transmisión, clasificación y destrucción.
	P4	**Acuerdos con otras organizaciones** Constatar que los acuerdos con otras organizaciones que compartan información deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.
Documentos por revisar	D1	Acuerdos de información compartida.
	D2	Registro de etiquetas de información de la organización.

4.4. DOMINIO 8: Seguridad en Recursos Humanos

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.1.**	**Seguridad antes del empleo**
Control	**8.1.1.**	**Inclusión de la seguridad en las responsabilidades y funciones laborales**
Objetivo	Definir y documentar las funciones y responsabilidades de los empleados, contratistas y terceros en concordancia con la política de seguridad de la organización.	
Procedimientos Específicos	P1	**En concordancia con la política de seguridad de la organización** Verificar que las funciones y responsabilidades incluyan los siguientes requisitos: a) implementadas y realizadas en concordancia con la política de seguridad de la organización (véase el inciso 5.1). b) deben proteger a los activos de un acceso no autorizado, modificación, destrucción o interferencia. c) ejecutar procesos particulares o actividades. d) asegurar que la responsabilidad sea asignada al individuo para tomar acciones. e) reportar eventos de seguridad o eventos potenciales u otro riesgo de seguridad para la organización.
	P2	**Definición y comunicación a candidatos.** Constatar que las funciones de seguridad y de responsabilidad son definidas y comunicadas claramente a los candidatos al trabajo durante el proceso de selección
	P3	**Individuos no relacionados con el proceso de selección.** Constatar que las funciones de seguridad y de responsabilidad para individuos no relacionados con el proceso de selección de la organización, como por ejemplo los que se encuentran comprometidos a través de una organización de terceros, sean claramente definidas y comunicadas.
Documentos por revisar	D1	Documento de funciones y responsabilidades.
	D2	Documento de funciones y responsabilidades de terceros.
	D3	Registro de comunicación de funciones y responsabilidades a candidatos.

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.1.**	**Seguridad antes del empleo**
Control	**8.1.2.**	**Selección y política de personal**
Objetivo	Se debe llevar listas de verificación anteriores de todos los candidatos para empleo, contratistas y terceros en concordancia con las leyes, regulaciones y la ética, al igual que proporcionalmente a los requerimientos del negocio, la clasificación de la información ha ser acezada y los riesgos percibidos.	
Procedimientos Específicos	P1	**Definición de listas de verificación** Comprobar que las listas de verificación tomen en cuenta la privacidad, la protección de los datos del personal y/o el empleo basado en la legislación y además: a) la disponibilidad de referencias satisfactorias sobre actitudes, por ejemplo, una personal y otra de la organización. b) la comprobación (de los datos completos y precisos) del Curriculum Vitae del candidato c) la confirmación de las certificaciones académicas y profesionales d) una comprobación independiente de la identificación (con pasaporte o documento similar) e) comprobaciones mas detalladas, como criminales o de crédito.
	P2	**Selección a cargo de agencia** Comprobar la agencia (contratada para que brinde personal a la organización) especifique claramente sus responsabilidades en la selección, así como los procedimientos de notificación requeridos si las pruebas de selección no se han completado o si sus resultados son dudosos o preocupantes
	P3	**Acuerdos con terceros** Verificar que los acuerdos con terceros especifiquen claramente las responsabilidades y los procedimientos notificados para la selección.
	P4	**Recolección y maniobra de información de candidatos según ley** Constatar que la información de todos los candidatos que han sido considerados para posiciones en la organización son recolectados y maniobrados en concordancia con cualquier legislación apropiada y existente en la jurisdicción relevante.
Documentos por revisar	D1	Acuerdos con agencias terceras.
	D2	Legislación acerca de contrato de personal.
	D3	Listas de verificación

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.1.**	**Seguridad antes del empleo**
Control	**8.1.3.**	**Acuerdos de confidencialidad**
Objetivo	Como parte de su obligación contractual, empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones del contrato de empleo el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	
Procedimientos Específicos	P1	**Términos y condiciones del empleo.** Los términos y condiciones reflejan la política de organización, además de aclarar y establecer: a) que todos los empleados, contratistas y terceros a los que se les ha dado acceso a información sensible deben firmar un acuerdo de confidencialidad y de no divulgación antes de darle el acceso a las instalaciones de procesamiento de información. b) las responsabilidades y derechos del contratista de empleados o cualquier otro usuario, por ejemplo en relación con la legislación de la protección de las leyes o de los datos del derecho del autor. c) las responsabilidades para la clasificación de la información y la gestión de los activos organizacionales asociados con los sistemas de información y los servicios maniobrados por el empleado, contratista o tercero (véase también 7.2.1 y 10.7.3). d) las responsabilidades del empleado, contratista o terceros para maniobrar la información recibida de otras compañías o terceros. e) las responsabilidades de la organización para maniobrar información personal, incluyendo información creada como resultado del empleo en la organización. f) las responsabilidades que son extendidas fuera de las premisas de la organización y fuera del periodo normal del trabajo, como por ejemplo en el caso del trabajo en casa, (véase también 9.2.5 y 11.7.1). g) las acciones ha ser tomadas si el empleado, contratista o tercero no cumple con los requisitos de seguridad de la organización (véase también 8.2.3).
	P2	**Aceptación de los términos y condiciones por empleados, contratistas y usuarios.** Verificar si la organización asegura que los empleados, contratistas y usuarios de terceros acepten los términos y condiciones referentes a la seguridad de información apropiada a la naturaleza y al grado de acceso que tendrán con los activos de la organización asociados los sistemas y a los servicios de información.
Documentos por revisar	D1	Códigos de conducta
	D2	Acuerdos contractuales con terceros.
	D3	Términos y condiciones para los diferentes puestos y cargos.

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.2.**	**Durante el empleo**
Control	**8.2.1.**	**Responsabilidades de la gerencia.**
Objetivo	La gerencia debe requerir empleados, contratistas y usuarios de terceros para aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.	
Procedimientos Específicos	P1	**Resumen de responsabilidades y roles** Verificar que la gerencia se asegure que los empleados, contratistas y terceros: a) cuenten con un resumen apropiado de sus responsabilidades y roles en la seguridad de información antes de garantizar el acceso a información sensible o a los sistemas de información. b) que estén provistos con una guía que establezca las expectativas de seguridad de su rol dentro de la organización. c) que se encuentren motivados de cumplir las políticas de seguridad de la organización. d) alcancen un nivel de conocimiento de seguridad relevante en sus roles y responsabilidades dentro de la organización (véase el inciso 8.2.2). e) que estén conforme con los términos y condiciones del empleo, los cuales incluyen la política de seguridad de información de la organización y métodos apropiados de trabajo. f) continúen teniendo habilidades y calificaciones apropiadas.
	P2	**Motivar al personal** Constatar que la gerencia mantenga motivados a su personal.
Documentos por revisar	D1	Documentos de términos y condiciones de los empleos.
	D2	Política de Seguridad de información
	D3	Guía de expectativa de seguridad de cada rol dentro de la organización

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.2.**	**Durante el empleo**
Control	**8.2.2.**	**Conocimiento, educación y entrenamiento de la seguridad de información**
Objetivo	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	
Procedimientos Específicos	P1	**Entrenamiento en el conocimiento** Constatar que el entrenamiento en el conocimiento empieza con una inducción formal del proceso designado para introducir la política de seguridad de la organización y las expectativas.
	P2	**Entrenamiento en curso** Verificar que el entrenamiento en curso incluye requisitos de seguridad, responsabilidades legales y controles del negocio.
Documentos por revisar	D1	Documento de requisitos de seguridad

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.2.**	**Durante el empleo**
Control	**8.2.3.**	**Proceso disciplinario**
Objetivo	Existencia de un proceso formal disciplinario para empleados que han cometido una apertura en la seguridad.	
Procedimientos Específicos	P1	**Verificación de apertura en la seguridad** Verificar previamente que la apertura en la seguridad ha ocurrido antes de comenzar el proceso disciplinario.
	P2	**Tratamiento de los empleados** Comprobar que se sigue un correcto y justo tratamiento de los empleados que son sospechosos de cometer aperturas en la seguridad.
	P3	**Respuesta del proceso disciplinario** Constatar que el proceso formar disciplinario provee una respuesta graduada que tome en consideración factores como la naturaleza, la gravedad de la apertura y su impacto en el negocio, si es que la ofensa es repetida o única o si es que el violador estuvo propiamente entrenado, leyes relevantes, contratos de negocio así como otros factores si son requeridos.
	P4	**Casos serios de mala conducta.** Constatar que, en casos serios de mala conducta, el proceso permite el retiro de sus labores, derechos de acceso y privilegios así como una escolta inmediata fuera del sitio, si es que es necesario.
Documentos por revisar	D1	Políticas y procedimientos organizacionales de seguridad.
	D2	Leyes según el tipo de mala conducta.
	D3	Contratos con empleados.
	D4	Reportes de sistemas (logs)
	D5	Procedimientos del proceso disciplinario
	D6	Documento del proceso disciplinario

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.3.**	**Finalización o cambio de empleo**
Control	**8.3.1.**	**Responsabilidades de finalización**
Objetivo	Definir y asignar las responsabilidades para realizar la finalización de un empleo o el cambio de este.	
Procedimientos Específicos	P1	**Comunicación de la finalización** Verificar que la finalización de las responsabilidades incluyen requisitos de seguridad en curso y responsabilidades legales y donde sea apropiado, responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad (véase el inciso 6.1.5.) y términos y condiciones (véase 8.1.3.) continuas por un periodo definido después del término del contrato de empleo o de terceros.
	P2	**Responsabilidades y tareas después de la finalización** Verificar que en el contrato de empleo o en los contratos de terceros estén contenidas las responsabilidades y tareas que son todavía válidas después de la finalización del empleo.
	P3	**Manejo de cambios de responsabilidad o empleo** Verificar que los cambios de responsabilidad o empleo sean maniobrados como la finalización de la respectiva responsabilidad o empleo y la nueva responsabilidad o empleo sea controlada como se describe en 8.1.
Documentos por revisar	D1	Funciones de Recursos Humanos.
	D2	Procedimientos de seguridad relevantes.
	D3	Procedimientos de finalización de responsabilidades.
	D4	Términos y condiciones del contrato con empleados, contratistas y terceros.

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.3.**	**Finalización o cambio de empleo**
Control	**8.3.2.**	**Retorno de activos**
Objetivo	Todos los empleados, contratistas y terceros deben retornar todos los activos de la organización que estén en su posesión hasta la finalización de su empleo, contrato o acuerdo.	
Procedimientos Específicos	P1	**Formalización del retorno de activos en el proceso de finalización** Comprobar que el proceso de finalización es formalizado para incluir el retorno previo de los software, documentos corporativos y equipos. Otros activos de la organización como dispositivos móviles de cómputo, tarjetas de crédito, tarjetas de acceso, manuales e información guardada en medios electrónicos, también necesitan ser devueltos.
	P2	**Uso de equipos personales o equipos comprados a la organización** Comprobar que, en caso donde el empleado/contratista/tercero compra el equipo de la organización o usa su propio equipo, se siga procedimientos para asegurar que toda la información relevante es transferida a la organización y borrado con seguridad del equipo (véase 10.7.1.)
	P3	**Documentación y transferencia de conocimientos.** En casos donde un empleado, contratista o tercero tiene conocimiento que es importante para las operaciones en curso, verificar que esa información se documente y transfiera a la organización
Documentos por revisar	D1	Registros de activos asignados al empleado
	D2	Reporte de retorno de activos asignados al empleado.
	D3	Documentación de información relevante de conocimientos sobre operaciones en curso.
	D4	Registros de activos propios del empleado
	D5	Registros de información compartida en los activos propios del empleado.

Dominio	**8.**	**SEGURIDAD EN RECURSOS HUMANOS**
Categoría	**8.3.**	**Finalización o cambio de empleo**
Control	**8.3.3.**	**Retiro de los derechos de acceso.**
Objetivo	Remover los derechos de acceso para todos los empleados, contratistas o usuario de terceros a la información y a las instalaciones del procesamiento de información hasta la culminación del empleo, contrato o acuerdo, o debe ser ajustada en caso de cambio.	
Procedimientos Específicos	P1	**Reconsideración de derechos de acceso.** Verificar que hasta la culminación, se reconsidere los derechos de acceso de un individuo a los activos asociados con los sistemas de información y a los servicios.
	P2	**Retiro de todos los derechos de acceso no aprobados** Verificar que los cambios en un empleo se reflejen en el retiro de todos los derechos de acceso que no fueron aprobados para el nuevo empleo, incluyendo acceso lógico y físico, llaves, tarjetas de identificación, instalaciones del proceso de información (véase 11.2.4.), suscripciones y retiro de cualquier documentación que los identifica como miembro actual de la organización
	P3	**Conocimiento de contraseñas a activos.** Si un empleado, contratista o usuario tercero saliente ha sabido contraseñas para activos restantes de las cuentas, verificar el cambio de las mismas hasta la finalización o cambio del empleo, contrato o acuerdo.
	P2	**Retiro de accesos a activos de información y equipos.** Constatar que los derechos a acceso para activos de información y equipos sean reducidos o removidos antes que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo como: a) si la finalización o cambio es iniciado por el empleado, contratista o usuario de tercero, o por la gerencia y la razón de la finalización. b) las responsabilidades actuales del empleado u otro usuario. c) el valor de los activos a los que se accede actualmente.
Documentos por revisar	D1	Derechos de acceso otorgados a empleados, contratistas y/o terceros.
	D2	Responsabilidades y funciones de empleados o usuarios

4.5. DOMINIO 9: Seguridad Física y del entorno

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.1.**	**Perímetro de seguridad física**
Objetivo	Usar los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción para proteger áreas que contengan información y recursos de procesamiento de información	
Procedimientos Específicos	P1	**Definir perímetro de seguridad** Verificar que el perímetro de seguridad está claramente definido y el lugar y fuerza de cada perímetro depende de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos.
	P2	**Solidez física** Comprobar que el perímetro de un edificio o un lugar que contenga recursos de tratamiento de información tiene solidez física.
	P3	**Área de recepción manual** Comprobar que exista un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso restringe solo al personas autorizado.
	P4	**Barreras físicas** Verificar que existen barreras físicas extendidas desde el suelo real al techo real.
	P5	**Puerta para incendios** Constatar que las puertas para incendios y del perímetro de seguridad tienen alarma, que son monitoreadas y probadas en conjunción con las paredes.
	P6	**Detección de intrusos** Verificar la instalación de sistemas adecuados de detección de intrusos e acuerdo a estándares regionales, nacionales o internacionales.
Documentos por Revisar	D1	Documento de seguridad física
	D2	Mapas de ubicación de barreras físicas
	D3	Documento de ubicación de puertas para incendios.

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.2.**	**Controles físicos de entradas**
Objetivo	Proteger las áreas de seguridad por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado	
Procedimientos Específicos	P1	**Supervisar visitas a las áreas seguras** Verificar que se supervise las visitas a las áreas seguras, a menos que el acceso haya sido aprobado previamente, y se deba registrar la fecha y momento de entrada y salida.
	P2	**Acceso a información sensible** Comprobar que se controla y restringe solo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento.
	P3	**Personal identificado visiblemente** Constatar que se exija a todo el personas que lleve puesta alguna forma de identificación visible y se le solicite a los extraños no acompañados y a cualquier que no lleve dicha identificación visible, que se identifique
	P4	**Acceso de terceros** Verificar que se garantice el acceso restringido al personal de apoyo de terceros, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando sea requerido.
	P5	**Revisar y actualizar derechos de acceso** Comprobar que se revisan y actualizan regularmente los derechos de accesos a las áreas de seguridad (véase 8.3.3.)
Documentos por revisar	D1	Registro de entrada/salida de personas en áreas seguras.
	D2	Documento de derechos de accesos a áreas de seguridad
	D3	Responsabilidades del personal

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.3.**	**Seguridad de oficinas, despachos y recursos**
Objetivo	Aginar y aplicar la seguridad para oficinas, despachos y recursos.	
Procedimientos Específicos	P1	**Regulaciones y estándares de salud y seguridad** Verificar que se tomó en cuenta las regulaciones y estándares de salud y seguridad.
	P2	**Equipos con clave** Verificar que se instalan equipos con clave para evitar el acceso al público
	P3	**Mínima indicación del propósito del edificio** Comprobar que los edificios sean discretos y dan una mínima indicación de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información.
	P4	**No accesibilidad de directorios telefónicos internos** Constatar que los directorios y las guías telefónicas internas identificando locaciones de los recursos de información sensible no son fácilmente accesibles por el público.
Documentos por revisar	D1	Regulaciones y estándares de salud y seguridad
	D2	Procedimientos de acceso y uso a directorios telefónicos internos
	D3	Procedimientos de rotulación de activos e infraestructura

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.4.**	**Protección contra amenazas externas y ambientales**
Objetivo	Designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.	
Procedimientos Específicos	P1	**Premisas vecinas** Comprobar que se consideró cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.
	P2	**Evitar daños** Verificar que se consideraron las siguientes pautas para evitar daño por parte del fuego, inundación, temblores, explosiones, malestar civil y otras formas de desastre natural o humana: a) los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante de las áreas seguras. No se deberían almacenar dentro de un área segura suministros a granel hasta que se necesiten. b) el equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal c) equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente.
Documentos por revisar	D1	Documentos de riesgos de entidades vecinas.
	D2	Documento de Análisis de riesgo.

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.5.**	**El trabajo en las áreas seguras**
Objetivo	Diseñar y aplicar protección física y pautas para trabajar en áreas seguras.	
Procedimientos Específicos	P1	**Conocer la existencia de un área segura si lo necesitara para su trabajo** Verificar que solo el personal que necesitara para su trabajo una zona segura, debe conocer la existencia de ésta.
	P2	**Evitar trabajos no supervisados** Verificar que se evita el trabajo no supervisado en áreas seguras tanto por motivos de salud como para evitar oportunidades de actividades maliciosas.
	P3	**Control de áreas seguras** Constatar que las áreas seguras estén cerradas y controlarse periódicamente cuando estén vacías. Verificar la prohibición de presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.
Documentos por revisar	D1	Documento de especificación las áreas seguras.
	D2	Procedimientos de trabajos en áreas seguras.
	D3	Controles en áreas seguras.

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.1.**	**Áreas seguras**
Control	**9.1.6.**	**Acceso público, áreas de carga y descarga**
Objetivo	Controlar las áreas de carga y descarga, aislarse de los recursos de tratamiento de información para evitar accesos no autorizados.	
Procedimientos Específicos	P1	**Controles para las áreas de carga y descarga** Verificar la consideración de las siguiente pautas: a) se deberían restringir los accesos al área de carga y descarga desde el exterior únicamente al personal autorizado e identificado. b) el área de carga y descarga se debería diseñar para que los suministros puedan descargarse sin tener acceso a otras zonas del edificio. c) la puerta externa del área debería estar cerrada cuando la interna esté abierta. d) el material entrante se debería inspeccionar para evitar posibles amenazas segregadas antes de llevarlo a su lugar de utilización. e) el material entrante se debería registrar en concordancia con los procedimientos de gestión de activos (véase el inciso 7.1.1) al entrar en el lugar. f) el material entrante y saliente debería ser físicamente separado, donde sea posible.
Documentos por revisar	D1	Procedimientos de carga y descarga en zonas seguras.
	D2	Políticas de acceso público

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.1.**	**Instalación y protección de equipos**
Objetivo	Proteger los equipos para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados	
Procedimientos Específicos	P1	**Sitio de equipos** Verificar que los equipos se sitúen donde se minimicen los accesos innecesarios a las áreas de trabajo
	P2	**Instalación de equipos de tratamiento y almacenamiento de información** Verificar que los equipos de tratamiento y almacenamiento de información que manejen datos sensibles se instalen dónde se reduzca el riesgo de que personas no autorizadas vean los procesos durante su uso
	P3	**Equipos con protección especial** Constatar que los elementos que requieran especial protección se aíslen para reducir el nivel general de protección requerido
	P4	**Controles** Verificar que los controles son adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo.
	P5	**Fumar, beber y comer cerca de equipos** Constatar que la organización incluye en su política cuestiones sobre fumar, beber y comer cerca de los equipos de tratamiento de información
	P6	**Condiciones ambientales** Constatar que se vigilan las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información
	P7	**Protección contra la luz** Verificar que la protección contra la luz se aplica a todos los edificios y ajustan filtros de luz a todas las líneas de poder y de comunicación
	P8	**Protección especial para ciertos equipos** Verificar que para los equipos situados en ambientes industriales se consideran el uso de métodos de protección especial (por ejemplo cubiertas para teclados)
	P9	**Protección para evitar pérdidas de información** Comprobar que el equipo que procesa información sensible es protegido con el fin de minimizar el riesgo de pérdidas de información

Documentos por revisar	D1	Mapa de ubicación de equipos y justificativas
	D2	Documento especificando los equipos de protección especial.
	D3	Controles físicos para los equipos
	D4	Políticas de comportamiento del personas sobre alimentos en el lugar de trabajo

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.2.**	**Suministro eléctrico**
Objetivo	Proteger los equipos contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo.	
Procedimientos Específicos	P1	**Instalaciones adecuadas** Comprobar que todas las instalaciones de apoyo, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado sean adecuados para los sistemas que están apoyando.
	P2	**Inspección y aprobación de equipos de apoyo** Comprobar que los equipos de apoyo sean inspeccionados regularmente y probados apropiadamente para asegurar su funcionamiento apropiado y para reducir cualquier riesgo causado por su mal funcionamiento o por una falla.
	P3	**Sistemas de Alimentación Ininterrumpida (UPS)** Constatar la instalación del UPS para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio.
	P4	**Instalaciones y conexiones de emergencia** Verificar la instalación de interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se dispone de alumbrado de emergencia.
	P5	**Suministro de agua** Comprobar que el suministro de agua es estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados).
	P6	**Equipos de telecomunicación** Comprobar que los equipos de telecomunicación están conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio es adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.
Documentos por revisar	D1	Contratos con proveedores de servicios.
	D2	Documentos de instalaciones de alimentación de servicios.
	D3	Instalaciones y conexiones para emergencias

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.3.**	**Seguridad del cableado**
Objetivo	Proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.	
Procedimientos Específicos	P1	**Líneas de energía y telecomunicaciones** Constatar que las líneas de energía y telecomunicaciones en las zonas de tratamiento de información, están enterradas, cuando sea posible, o se han adoptado medidas alternativas de protección
	P2	**Protección de la red cableada** Constatar que la red cableada se protege contra intercepciones no autorizadas o daños, por ejemplo, uso de conductos y evitando rutas a través de áreas públicas
	P3	**Separar cables de energía de los de comunicaciones** Verificar que están separados los cables de energía de los de comunicaciones.
	P4	**Identificación de cables** Verificar el uso de cables claramente identificados y marcas de equipo con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta.
	P5	**Lista documentada de parches** Verificar el uso de una lista documentada de parches con el fin de reducir la posibilidad de errores.
	P6	**Sistemas sensibles o críticos** Comprobar la consideración de medidas adicionales para sistemas sensibles o críticos como: 1) instalación de conductos blindados y cajas o salas cerradas en los puntos de inspección y terminación. 2) uso de rutas o de medios de transmisión alternativos. 3) uso de cableado de fibra óptica. 4) uso de un escudo electromagnético para proteger los cables. 5) inicialización de inspecciones físicas y técnicas a los dispositivos no autorizados adjuntados a los cables. 6) acceso controlado para parchar paneles y cuartos de cable.
Documentos por revisar	D1	Mapa de redes de cableado.
	D2	Documento de parches de red de cableado.
	D3	Documento de sistemas sensible o críticos
	D4	Procedimientos para la protección de la red cableada

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.4.**	**Mantenimiento de equipos**
Objetivo	Mantener los equipos adecuadamente para asegurar su continuidad e integridad	
Procedimientos Específicos	P1	**Mantenimiento de equipos** Constatar que los equipos se mantienen de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador
	P2	**Reparación y servicio de los equipos** Corroborar que sólo el personal de mantenimiento debidamente autorizado realiza la reparación y servicio de los equipos
	P3	**Documentar los fallos y mantenimientos** Comprobar que se registran documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo
	P4	**Implementación de controles en mantenimientos** Verificar la implementación de controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo a la organización; donde sea necesario, se despeja la información sensible del equipo.
	P5	**Cumplimiento de requisitos** Comprobar que se cumplen todos los requisitos impuestos por las políticas de los seguros.
Documentos por revisar	D1	Especificaciones de servicio del suministrados
	D2	Documento de mantenimiento de equipos.
	D3	Funciones y capacidades del personal de reparación y servicio.
	D4	Controles para el mantenimiento a un equipo

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.5**	**Seguridad de equipos fuera de los locales de la organización**
Objetivo	Aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización tomando en cuenta los diversos riesgos a los que está expuesto.	
Procedimientos Específicos	P1	**Autorización de gerencia** Comprobar que sólo la gerencia puede autorizar el uso de cualquier equipo para tratamiento de información fuera de los locales de la organización, sea quien sea su propietario.
	P2	**Equipos fuera de las instalaciones** Constatar que los equipos y medios que contengan datos con información y sean sacados de su entorno habitual no se dejan desatendidos en sitios públicos. Cuando viajen, los computadores portátiles se transportan de una manera disimulada como equipaje de mano.
	P3	**Instrucciones del fabricante** Verificar que se observan siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos
	P4	**Controles para el trabajo en el domicilio** Constatar que los controles para el trabajo en el domicilio se determinan mediante una evaluación de los riesgos y se aplican los controles convenientes según sea apropiado, por ejemplo, en controles de acceso a los computadores, una política de puesto de trabajo despejado y cierre de las zonas de archivo (véase también ISO/IEC 18028 Seguridad de Redes)
	P5	**Seguro para equipos** Verificar la existencia de un seguro adecuado que cubra los equipos fuera de su lugar de trabajo.
	P6	**Ubicación** Los riesgos de seguridad, por ejemplo, de daño, robo y escucha, pueden variar mucho según la ubicación. Verificar que se tiene en cuenta al determinar los controles más apropiados.
Documentos por revisar	D1	Autorizaciones otorgadas/denegadas por gerencia
	D2	Procedimientos de usuarios para manejo de equipos fuera de las instalaciones
	D3	Documento de uso de equipos para el trabajo en el domicilio
	D4	Análisis de riesgos de la ubicación del edificio de la empresa y domicilios de los empleados.
	D5	Contrato de seguros para equipos

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.6.**	**Seguridad en el rehúso o eliminación de equipos**
Objetivo	Todos los elementos del equipo que contengan dispositivos de almacenamiento deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.	
Procedimientos Específicos	P1	**Destrucción física de los dispositivos de almacenamiento** Verificar que se eliminan los dispositivos de almacenamiento con información sensible usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.
	P2	**Evaluación de riesgos** Verificar que los dispositivos dañados que contienen data sensible requieren una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.
Documentos por revisar	D1	Procedimientos para la eliminación de dispositivos de almacenamiento
	D2	Documento de evaluación de riesgos de dispositivos dañados.

Dominio	**9.**	**SEGURIDAD FÍSICA Y DEL ENTORNO**
Categoría	**9.2.**	**Seguridad de los equipos**
Control	**9.2.7.**	**Retiro de la propiedad**
Objetivo	El equipo, información o software no debe ser sacado fuera del local sin autorización.	
Procedimientos Específicos	P1	**Autorización** Verificar que el equipo, información o software no es sacado fuera del local sin autorización
	P2	**Identificación de autoridades** Verificar que los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos son claramente identificados
	P3	**Limites de tiempo** Verificar que los tiempos limite para el retiro de equipos son fijados y el retorno del equipo verificado para asegurar la conformidad
	P4	**Registro del equipo** Verificar que el equipo es registrado, si es necesario y apropiado, cuando es removido fuera del local así como cuando es devuelto.
Documentos por revisar	D1	Procedimientos para el ingreso y egreso de activos de información de la organización
	D2	Documento de autoridades que permiten el ingreso y salida de activos de información.

4.6. DOMINIO 10: Gestión de comunicaciones y operaciones

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.1.**	**Procedimientos y responsabilidades de operación**
Control	**10.1.1.**	**Documentación de procedimientos operativos**
Objetivo	Documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran	
Procedimientos Específicos	P1	**Procedimientos para actividades del sistema (procesamiento de información y recursos de comunicación)** Verificar que se prepararon los procedimientos documentados para actividades del sistema asociados con el procesamiento de información y los recursos de comunicación, como los procedimientos de prendido y apagado de la computadora, backups, mantenimiento de equipos, manipulación de medios, ambientes de computo y manipulación de correos, y seguridad. Se consideró lo siguiente: a) el proceso y utilización correcta de la información. b) backup (véase el inciso 10.5). c) los requisitos de planificación, incluyendo las interdependencias con otros sistemas, con los tiempos de comienzo más temprano y final más tardío posibles de cada tarea. d) las instrucciones para manejar errores u otras condiciones excepcionales que puedan ocurrir durante la tarea de ejecución, incluyendo restricciones en el uso de servicios del sistema (véase el inciso 11.5.4). e) los contactos de apoyo en caso de dificultades inesperadas operacionales o técnicas. f) las instrucciones especiales de utilización de resultados, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de destrucción segura de resultados producidos como consecuencia de tareas fallidas (véase también 10.7.2 y 10.7.3). g) el reinicio del sistema y los procedimientos de recuperación a utilizar en caso de fallo del sistema. h) la gestión de la información del rastro de auditoria y del registro de sistema (véase 10.10.).
	P2	**Procedimientos para actividades de administración del sistema** Comprobar la preparación de procedimientos documentados para las actividades de administración del sistema y cualquier cambio que se realice debe ser autorizado por la gerencia. Donde sea técnicamente viable, los sistemas de información se gestiona consistentemente usando los mismos procedimientos, herramientas y recursos
Documentos por revisar	D1	Procedimientos para administración del sistema
	D2	Procedimientos para procesamiento de información
	D3	Procedimientos para los recursos de comunicación

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.1.**	**Procedimientos y responsabilidades de operación**
Control	**10.1.2.**	**Gestión de cambios**
Objetivo	Controlar los cambios en los sistemas y recursos de tratamiento de información	
Procedimientos Específicos	P1	**Control de gestión de cambios** Verificar que los sistemas operacionales y los software de aplicación están sujetos a un estricto control de la gestión de cambios. Además se considera: a) la identificación y registro de cambios significativos. b) planeamiento y prueba de los cambios. c) la evaluación de los posibles impactos, incluyendo impactos de seguridad, de dichos cambios. d) un procedimiento formal de aprobación de los cambios propuestos. e) la comunicación de los detalles de cambio a todas las personas que corresponda. f) procedimientos que identifiquen las responsabilidades de abortar y recobrarse de los cambios sin éxito y de acontecimientos imprevistos.
	P2	**Responsabilidades y procedimientos de gestión de cambios.** Comprobar la implantación responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos.
	P3	**Cambios en los programas** Constatar que cuando se cambien los programas se conserve un registro de auditoria conteniendo toda la información importante.
Documentos por revisar	D1	Documento de gestión de cambios
	D2	Responsabilidades y procedimientos de gestión de cambios.
	D3	Informes de auditorías.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.1.**	**Procedimientos y responsabilidades de operación**
Control	**10.1.3.**	**Segregación de tareas.**
Objetivo	Segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización.	
Procedimientos Específicos	P1	**Acceso, modificación o utilización de activos** Verificar que se tiene cuidado de que cualquier persona puede acceder, modificar o utilizar los activos sin autorización o sin ser detectado
	P2	**Iniciación de evento es diferente a autorización.** Verificar que la iniciación de un evento debe estar separada de su autorización.
	P3	**Confabulación** Verificar la existencia de la posibilidad de confabulación es considerada en el diseño de los controles.
Documentos por revisar	D1	Documento de segregación de tareas
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.1.**	**Procedimientos y responsabilidades de operación**
Control	**10.1.4.**	**Separación de los recursos para desarrollo y para producción**
Objetivo	La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.	
Procedimientos Específicos	P1	**Controles para el nivel de separación entre entornos.** Comprobar la identificación e implementación de controles adecuados para el nivel de separación entre los entornos de desarrollo, prueba y producción que es necesario para evitar problemas operacionales. Se considera lo siguiente: a) las reglas de transferencia del software desde un estado de desarrollo al de producción deben ser definidos y documentados. b) el software de desarrollo y el de producción deberían, si es posible, funcionar en procesadores diferentes, o en dominios o directorios distintos. c) los compiladores, editores y otros servicios del sistema no deberían ser accesibles desde los sistemas de producción, cuando no se necesiten. d) el entorno de prueba del sistema debe emular el entorno del sistema operacional lo mas cercano posible. e) los usuarios deben utilizar diferentes perfiles de usuario para los sistemas operacionales y de prueba; y los menús deben exhibir mensajes de identificación apropiados con el fin de reducir el riesgo por error. f) los datos sensibles no deben ser copiados en el entorno del sistema de prueba.
Documentos por revisar	D1	Documento de controles para el nivel de separación de entornos.
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.2.**	**Gestión de servicios externos**
Control	**10.2.1.**	**Servicio de entrega**
Objetivo	Asegurar que todos los controles de seguridad, definiciones de servicio y niveles de entrega incluida en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.	
Procedimientos Específicos	P1	**Arreglos de seguridad** Verificar que el servicio entregado por terceros incluye los arreglos de seguridad acordados, definiciones de servicio y aspectos de la gestión del servicio.
	P2	**Outsourcing** Comprobar, en caso de arreglos de outsourcing, que se planee las transiciones (de información, recursos del procesamiento de información y cualquier otra cosa que requiere ser movido), y que la seguridad se mantiene a través del periodo de transición.
	P3	**Capacidad suficiente de terceros** Verificar que la organización se asegure que los terceros mantengan una capacidad suficiente junto con planes realizables designados para asegurar que los niveles continuos del servicio acordado sean mantenidos siguiendo fallas mayores del servicio o desastre (véase 14.1).
Documentos por revisar	D1	Contratos con terceros sobre seguridad
	D2	Constancia de capacidad suficiente por parte de terceros.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.2.**	**Gestión de servicios externos**
Control	**10.2.2.**	**Monitoreo y revisión de los servicios externos**
Objetivo	Monitorear y revisar regularmente los servicios, reportes y registros provistor por terceros. Las auditorias se llevan a cabo regularmente.	
Procedimientos Específicos	P1	**Aseguramiento adhesión** Verificar que el monitoreo y la revisión de los servicios externos aseguran que todos los términos de seguridad de la información y las condiciones de los acuerdos han sido adheridos y, que los incidentes y problemas en la seguridad de información han sido manejados propiamente. Esto implica una relación y proceso de gestión del servicio entre la organización y terceros para: a) servicio de monitoreo de niveles de funcionamiento para verificar que se adhieran a los acuerdos. b) reportes de revisión de servicio producidos por terceros y que arregle reuniones regulares de progreso como requieran los acuerdos c) proveer información acerca de los incidentes de seguridad de información y revisión de esta información por terceros y la organización como requiera los acuerdos y cualquier pautas de apoyo y procedimientos. d) revisar los acuerdos y los rastros de intervención de los eventos de seguridad, problemas operacionales, fallas, trazabilidad de faltas e interrupciones relacionadas con el servicio entregado. e) resolver y manejar cualquier problema identificado.
	P2	Comprobar que la responsabilidad para manejar las relaciones con un tercero es asignado a un individuo designado o a un equipo de gestión de servicio.
	P3	Constatar que la organización asegure que los proveedores externos asignen responsabilidades para verificar la conformidad y el cumplimiento de los requisitos de los acuerdos
	P4	Constatar la disponibilidad de habilidades y recursos suficientes para monitorear los requisitos de los acuerdos (véase 6.2.3.), en particular los requisitos de seguridad de información.
	P5	Verificar que se toman acciones apropiadas cuando se observan deficiencias en el servicio entregado.
	P6	Verificar el mantenimiento de un control y una visión general suficiente en todos los aspectos para información sensible o crítica o a los recursos del procesamiento de información accedidos, procesados o gestionado por terceros.
Documentos por revisar	D1	Acuerdos firmados con terceros
	D2	Procedimientos en caso de deficiencias en el servicio entregado.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.2.**	**Gestión de servicios externos**
Control	**10.2.3.**	**Gestionando cambios para los servicios externos**
Objetivo	Cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes.	
Procedimientos Específicos	P1	**Cambios realizados por la organización para implementar** Verificar que se tome en cuenta para el proceso de gestión de cambios para los servicios externos: 1) realces en el actual servicio ofrecido. 2) desarrollo de cualquier aplicación o sistema nuevo. 3) modificaciones o actualizaciones de las políticas y procedimientos organizacionales. 4) controles nuevos para resolver incidentes en la seguridad de información y para mejorar la seguridad.
	P2	**Cambios en los servicios externos para implementar** Verificar que se tome en cuenta para el proceso de gestión de cambios para los servicios externos: 1) cambios y realces en las redes. 2) el uso de nuevas tecnologías. 3) adopción de nuevos productos o versiones o lanzamientos nuevos. 4) nuevas herramientas y ambientes de desarrollo 5) cambios en la locación física de los recursos de servicio. 6) cambios en el vendedor.
Documentos por revisar	D1	Documento de gestión de servicios externos.
	D2	Documento de política de seguridad de información.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.3.**	**Planificación y aceptación del sistema**
Control	**10.3.1.**	**Planificación de la capacidad**
Objetivo	El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido.	
Procedimientos Específicos	P1	Comprobar que se identifican los requisitos de capacidad para cada actividad que se esté llevando a cabo o para cada actividad nueva.
	P2	Verificar que se aplicar el monitoreo de los sistemas.
	P3	Comprobar la instalación de controles de detección para detectar los problemas en un tiempo debido.
	P4	Verificar que la gerencia monitorea la utilización de los recursos claves del sistema.
	P5	Verificar que se identifica las tendencias de uso, particularmente relativas a las aplicaciones del negocio o las herramientas de administración de sistemas de información.
	P6	Constatar que los administradores usan las tendencias de uso para identificar y evitar posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios del usuario, y para planificar la accion correctora apropiada.
Documentos por revisar	D1	Reportes de tendencias de uso
	D2	Documento de implementación de controles de detección

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.3.**	**Planificación y aceptación del sistema**
Control	**10.3.2.**	**Aceptación del sistema**
Objetivo	Se deberían establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deberían desarrollar con ellos las pruebas adecuadas antes de su aceptación.	
Procedimientos Específicos	P1	Verificar que los requisitos y criterios de aceptación de los nuevos sistemas están claramentes definidos, acordados, documentados y probados.
	P2	Constatar que los nuevos sistemas, actualizaciones y las nuevas versiones son migradas a producción solamente después de obtener una aceptación formal.
	P3	**Aceptación formal** Comprobar que se consideraron los siguitnes puntos antes de obtener la aceptación formal: a) los requisitos de rendimiento y capacidad de los computadores. b) los procedimientos de recuperación de errores y reinicio, así como los planes de contingencia. c) la preparación y prueba de procedimientos operativos de rutina según las normas definidas. d) un conjunto acordado de controles y medidas de seguridad instalados. e) manual de procedimiento eficaz. f) plan de continuidad del negocio como se requiere en el inciso 11.1. g) la evidencia de que la instalación del nuevo sistema no producirá repercusiones negativas sobre los existentes, particularmente en los tiempos con pico de proceso como a fin de mes. h) la evidencia de que se ha tenido en cuenta el efecto que tendrá el nuevo sistema en la seguridad global de la organización. i) la formación en la producción o utilización de los sistemas nuevos. j) la facilidad de empleo, como este afecta el funcionamiento del usuario y evita los errores humanos.
	P4	Comprobar que se realizaron pruebas apropiadas para confirmar que están satisfechas completamente todos los criterios de aceptación.
Documentos por revisar	D1	Documento de criterios de aceptación del sistema
	D2	Documentos de requisitos de aceptación del sistema.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.4.**	**Protección contra software malicioso**
Control	**10.4.1.**	**Medidas y controles contra software malicioso**
Objetivo	Se deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.	
Procedimientos específicos	P1	Verificar la existencia de una política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado (véase el inciso 15.1.2).
	P2	Constatar la existencia de una política formal de protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indicando las medidas protectoras a adoptar.
	P3	Verificar la realización de revisiones regulares del software y de los datos contenidos en los sistemas que soportan procesos críticos de la organización.
	P4	Verificar la existencia de la instalación y actualización frecuente de software de detección y reparación de virus, que exploren los computadores y los medios de forma rutinaria o como un control preventivo; las revisiones llevadas a cabo deben incluir: 1) verificación de archivos electrónicos de origen incierto o no autorizado, o recibidos a través redes no fiables, para comprobar la existencia de virus antes de usarlos. 2) verificación de todo archivo adjunto a un correo electrónico o de toda descarga para buscar software malicioso antes de usarlo. Esta comprobación se hará en distintos lugares, por ejemplo, en los servidores de correo, en los computadores personales o a la entrada en la red de la organización. 3) la verificación de códigos maliciosos en las páginas Web.
	P5	Verificar que existen los procedimientos y responsabilidades de administración para la utilización de la protección de antivirus, la formación para su uso, la información de los ataques de los virus y la recuperación de éstos (véanse los incisos 13.1 y 13.2).
	P6	Constatar que existen los planes de continuidad del negocio apropiados para recuperarse de los ataques de virus, incluyendo todos los datos y software necesarios de respaldo y las disposiciones para la recuperación (véase el capítulo 14)
	P7	Comprobar la implementación de procedimientos para recolectar información regularmente, como suscribirse a listas de correo y/o verificar paginas Web que contengan información sobre nuevos virus.
	P8	Constatar la existencia de los procedimientos para verificar toda la información relativa al software malicioso y asegurarse que los boletines de alerta son precisos e informativos. Los administradores aseguran que se diferencian los virus reales de los falsos avisos de virus, usando fuentes calificadas, por ejemplo, revistas reputadas, sitios de Internet fiables o los proveedores de software antivirus. Se advierte al personal sobre el problema de los falsos avisos de virus y qué hacer en caso de recibirlos.

Documentos por revisar	D1	Documento de controles contra software malicioso
	D2	Políticas de seguridad contra software malicioso

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.4.**	**Protección contra software malicioso**
Control	**10.4.2.**	**Medidas y controles contra código móvil**
Objetivo	Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe prevenir que este sea ejecutado.	
Procedimientos Específicos	P1	Verificar que se consideró, para protegernos contra acciones no autorizadas de códigos móviles, lo siguiente: a) ejecutar un código móvil en un ambiente lógico aislado. b) bloquear cualquier uso de código móvil. c) bloquear el recibo de código móvil. d) activar medidas técnicas como estén disponibles en un sistema especifico para asegurar que el código móvil esta manejado. e) controlar los recursos disponibles al acceso de código móvil. f) controlar criptográficamente para autentificar individualmente un código móvil.
Documentos por revisar	D1	Documento de procedimientos contra acciones no autorizadas de códigos móviles
	D2	Documento de política de seguridad de la organización

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.5.**	**Gestión de respaldo y recuperación**
Control	**10.5.1.**	**Recuperación de la información**
Objetivo	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.	
Procedimientos Específicos	P1	Verificar que se consideraron los siguientes puntos de la recuperación de información: a) se debería definir el nivel necesario de recuperación de la información. b) se debería almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación c) la extensión y frecuencia de los respaldos deben reflejar las necesidades de la organización, los requisitos de seguridad de la información envuelta, y la criticidad de la información para la operación continua de la organización. d) los respaldos deben estar almacenados en una locación remota, en una distancia suficiente para escapar de cualquier daño frente a un desastre en el local principal e) se debería dar a la información de respaldo un nivel adecuado de protección física y del entorno (véase el capítulo 9), un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo. f) los medios de respaldo se deberían probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia. g) se deberían comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación. h) en situaciones donde la confidencialidad sea importante, los respaldos deben ser protegidos por medios de encriptación.
Documentos por revisar	D1	Documento de procedimientos de recuperación de la información
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.6.**	**Gestión de seguridad en redes**
Control	**10.6.1.**	**Controles de red**
Objetivo	Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en transito.	
Procedimientos Específicos	P1	Verificar que la responsabilidad operativa de las redes está separada de la operación de los computadores si es necesario (véase 10.1.3.)
	P2	Verificar que se establecen responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios.
	P3	Comprobar que se establecen, si procede, controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados (véanse 11.4. y 12.3.) . También requiere controles y medidas especiales para mantener la disponibilidad de los servicios de las redes y de los computadores conectados.
	P4	Constatar que un registro y monitoreo apropiado sea aplicado para permitir el registro de acciones relevantes de seguridad
	P5	Comprobar que se coordine estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información
Documentos por revisar	D1	Documentos de controles de red
	D2	Documento de arquitectura de la red.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.6.**	**Gestión de seguridad en redes**
Control	**10.6.2.**	**Seguridad en los servicios de redes**
Objetivo	Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización.	
Procedimientos Específicos	P1	Constatar que la habilidad del proveedor del servicio de red para manejar servicios acordados de una manera segura son determinados y monitoreados regularmente, y el derecho para auditar es acordado.
	P2	Verificar que los acuerdos de seguridad necesarios para servicios particulares, como características de seguridad, niveles de servicio y los requisitos de gestión, son identificados. La organización asegura que los proveedores del servicio de red implementan estas medidas
Documentos por revisar	D1	Políticas de seguridad en los servicios de redes.
	D2	Acuerdos firmados con terceros.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.7.**	**Utilización de los medios de información**
Control	**10.7.1.**	**Gestión de medios removibles**
Objetivo	Debería haber procedimientos para la gestión de los medios informáticos removibles.	
Procedimientos Específicos	P1	Verificar que se documenta claramente todos los procedimientos y niveles de autorización
	P2	Constatar que se consideraron las siguientes pautas para la gestión de los medios removibles: a) se deberían borrar cuando no se necesiten más, los contenidos previos de todo medio reutilizable del que se desprenda la organización. b) donde sea necesario y práctico, todo medio desechado por la organización debería requerir autorización y se debería guardar registro de dicha remoción para guardar una pista de auditoría. c) todos los medios se deberían almacenar a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes d) la información almacenada en el medio, que requiere estar disponible mayor tiempo que el tiempo de vida del medio (en concordancia con las especificaciones del productor) debe ser también almacenada con el fin de no perder dicha información debido al deterioro del medio e) el registro de los medios removibles debe ser considerado para limitar la oportunidad de pérdida de datos f) los medios removibles deben ser solo activados si existe una razón de negocio para hacerlo.
Documentos por revisar	D1	Documento de procedimientos para la gestión de medios removibles
	D2	Documento de nivel de autorización para medios removibles

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.7.**	**Utilización de los medios de información**
Control	**10.7.2.**	**Eliminación de medios**
Objetivo	Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales.	
Procedimientos Específicos	P1	Constatar que se establecen procedimientos formales para minimizar el riesgo de filtro de información sensible a personas externas con la eliminación segura de los medios.
	P2	Verificar que los procedimientos para la seguridad de los medios que contienen información sensible son conmensurados con la sensibilidad de dicha información.
Procedimientos Específicos	P3	Verificar que se consideró los siguientes puntos: a) los medios que contengan información sensible se almacenarán y eliminarán de forma segura, por ejemplo, incinerándolos, triturándolos o vaciando sus datos para usarlos en otra aplicación dentro de la organización. b) los procedimientos deben permitir identificar los ítems que puedan requerir un dispositivo de seguridad. c) puede ser más fácil recoger y eliminar con seguridad todos los tipos de medios que intentar separar los que contienen información sensible. d) muchas organizaciones ofrecen servicios de recojo y eliminación de papel, equipos y medios. Debería cuidarse la selección de los proveedores adecuados según su experiencia y lo satisfactorio de los controles que adopten. e) se debería registrar la eliminación de elementos sensibles donde sea posible para mantener una pista de auditoría.
	P4	Comprobar que se considera el efecto de acumulación de medios a la hora de eliminar.
Documentos por revisar	D1	Procedimientos de eliminación de medios
	D2	Análisis de riesgos para los medios (eliminación)

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.7.**	**Utilización de los medios de información**
Control	**10.7.3.**	**Procedimientos de manipulación de la información.**
Objetivo	Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados.	
Procedimientos Específicos	P1	Constatar que se establezcan procedimientos de manipulación y almacenamiento de la información de forma coherente con su clasificación (véase 7.2.). Se considera los siguientes ítems: a) etiquetado en la administración de todos los medios. b) restricciones de acceso para identificar al personal no autorizado. c) mantenimiento de un registro formal de recipientes autorizados de datos. d) aseguramiento de que los datos de entrada, su proceso y la validación de la salida están completos. e) protección de los datos que están en cola para su salida en un nivel coherente con su criticidad. f) almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante. g) minimizar la distribución de datos. h) identificación clara de todas las copias de datos para su atención por el receptor autorizado. i) revisión de las listas de distribución y de receptores autorizados a intervalos regulares.
Documentos por revisar	D1	Documento de procedimientos de manipulación de la información
	D2	Documento de clasificación de información.

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.7.**	**Utilización de los medios de información**
Control	**10.7.4.**	**Seguridad de la documentación de sistemas**
Objetivo	Los documentación de sistemas debe ser protegida contra acceso no autorizado.	
Procedimientos Específicos	P1	Constatar que para proteger la documentación de sistemas de accesos no autorizados se considera lo siguiente: a) la documentación de sistemas se debería almacenar con seguridad. b) la lista de acceso a la documentación de sistemas se debería limitar al máximo, y ser autorizada por el propietario de la aplicación. c) la documentación de sistemas mantenida en una red pública, o suministrada vía una red pública, se debería proteger adecuadamente.
Documentos por revisar	D1	Procedimientos de seguridad de la documentación de los sistemas
	D2	Controles de seguridad para la documentación de los sistemas

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.8.**	**Intercambio de información**
Control	**10.8.1.**	**Políticas y procedimientos para el intercambio de información y software**
Objetivo	Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación.	
Procedimientos Específicos	P1	Constatar que los procedimientos y controles son seguidos cuando se utiliza instalaciones electrónicas de comunicación para el intercambio de información considera lo siguiente: a) los procedimientos designados para proteger la información intercambiada de una intercepción, copiado, modificación, cambio de ruta y destrucción. b) los procedimientos para la detección y protección contra código malicioso que puede ser transmitido a través del uso de comunicación electrónica (véase el inciso 10.4.1). c) los procedimientos para proteger información electrónica sensible que esta en forma de archivo adjunto. d) las políticas o pautas para el uso aceptable de las instalaciones de comunicación electrónica (véase el inciso 7.1.3). e) los procedimientos para el uso de comunicaciones inalámbricas, tomando en cuenta los riesgos particulares envueltos. f) las responsabilidades de los empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por difamación, hostigamiento, personificación, reenvío de cadenas de correos, compra no autorizada, etc. g) el uso de técnicas criptográficas como por ejemplo para proteger la confidencialidad, integridad y autenticidad de la información (véase el inciso 12.3). h) las pautas de disposición y retención para toda la correspondencia de negocios, incluyendo mensajes, en concordancia con la legislación y las regulaciones nacionales y locales. i) no dejar información critica o sensible en las instalaciones de impresión, como impresoras, copiadoras y faxes, ya que estas pueden ser acezadas por personal no autorizado. j) los controles y restricciones asociados con el reenvío de las instalaciones de comunicación como por ejemplo el reenvío automático de correos electrónicos a una dirección de correo externa. k) recordar al personal que deben de tomar precauciones como por ejemplo no revelar información sensible con el fin de evitar ser escuchado o interceptado cuando hagan una llamada telefónica mediante: 1) personas vecinas particularmente cuando se utiliza teléfonos móviles. 2) interceptación de teléfonos y otras formas de oír comunicaciones a través de acceso físico al equipo o a la línea telefónica, o utilizando equipos de recepción de escaneo. 3) personas al final del receptor.

		l) no dejar mensajes conteniendo información sensible en las maquinas contestadoras ya que estas pueden ser reproducidas por personas no autorizadas, guardadas en sistemas comunales o grabadas incorrectamente como resultado de un mal discado. m) recordar al personal sobre los problemas de usar las maquinas de fax, nombrando: 1) el acceso no autorizado para crear almacenes de mensajes con el fin de recuperarlos 2) la programación deliberada o accidentada de las maquinas para enviar mensajes a números específicos. 3) envío de documentos y mensajes a un número equivocado por un mal discado o por el uso de un numero mal grabado. n) recordar al personal no registrar datos demográficos, como la dirección de correo u otra información personal en cualquier software para evitar su uso no autorizado. o) recordar al personal que los fax modernos y las fotocopiadoras tienen paginas cache y paginas almacenadas en caso de que el papel se trabe y lo imprimirá una vez que se corrija el error.
Documentos por revisar	D1	Políticas de seguridad sobre conversaciones confidenciales en lugares públicos
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.8.**	**Intercambio de información**
Control	**10.8.2.**	**Acuerdos de Intercambio.**
Objetivo	Los acuerdos deben ser establecidos para el intercambio de información y software entre la organización y terceros.	
Procedimientos Específicos	P1	Constatar que los acuerdos de intercambio consideran las siguientes condiciones de seguridad: a) las responsabilidades de la gerencia para controlar y notificar la transmisión, despacho y recibo. b) procedimientos para notificar al que envía la transmisión, despacho o recibo. c) procedimientos para asegurar al trazabilidad y la no reproducción. d) estándares técnicos mínimos para empacado y transmisión. e) acuerdos de fideicomiso. f) estándares de identificación de mensajería. g) responsabilidades en los eventos de los incidentes de la seguridad de información como la perdida de datos h) uso de un sistema acordado de etiquetado para información sensible o critica, asegurando que los significados de las etiquetas sea entendido de inmediato y que la información sea protegida apropiadamente. i) las propiedades y responsabilidades de la protección de datos, copyright, conformidad de la licencia de software y consideraciones similares (véase 15.1.2 y 15.1.4). j) estándares técnicos para grabar y leer información y software; k) cualquier control especial que pueda ser requerido para proteger ítems sensibles como las llaves criptográficas (véase el inciso 12.3).
Documentos por revisar	D1	Documentos de acuerdos de intercambio.
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.8.**	**Intercambio de información**
Control	**10.8.3.**	**Medios físicos en tránsito**
Objetivo	Los medios conteniendo información deben ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los limites físicos de la organización.	
Procedimientos Específicos	P1	Verificar que aplican los siguientes controles y medidas para salvaguardar los medios informáticos transportados entre sedes: a) deberían usarse transportes o mensajeros fiables. b) debería convenirse entre las gerencias una lista de mensajeros autorizados. c) se debería realizar un procedimiento para comprobar la identificación de los mensajeros utilizados d) el envase debería ser suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito, de acuerdo con las especificaciones de los fabricantes, por ejemplo protegiéndonos contra cualquier factor ambiental que pueda reducir la efectividad de la restauración del medio como una exposición al calor, humedad o a campos electromagnéticos. e) deberían adoptarse controles especiales para proteger la información sensible de la divulgación o modificación no autorizadas, por ejemplo: 1) uso de contenedores cerrados. 2) entrega en mano. 3) envase con detección de apertura (que revela cualquier intento de acceso). 4) en casos excepcionales, fraccionamiento del envío en varías entregas que se envían por rutas diferentes.
Documentos por revisar	D1	Procedimientos de transporte de medios informáticos.
	D2	Documento de controles especiales para el transporte de medios informáticos

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.8.**	**Intercambio de información**
Control	**10.8.4.**	**Seguridad en la mensajería electrónica**
Objetivo	La información implicado con la mensajería electrónica debe ser protegida apropiadamente.	
Procedimientos Específicos	P1	Verificar que la seguridad para la mensajería electrónica incluye lo siguiente: a) protección de mensajes de accesos no autorizados, modificaciones o negación del servicio. b) asegurar una dirección y un transporte correcto del mensaje. c) confiabilidad y disponibilidad general del servicio. d) consideraciones legales, por ejemplo los requisitos para firmas electrónicas. e) obtención de aprobación antes de utilizar servicios externos públicos como mensajería instantánea o archivos compartidos. f) niveles más fuertes de autentificación del acceso de control de redes públicas accesibles.
Documentos por revisar	D1	Procedimientos para la seguridad en la mensajería electrónica
	D2	Documento de requisitos para firmas electrónicas

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.8.**	**Intercambio de información**
Control	**10.8.5.**	**Sistemas de Información de Negocios**
Objetivo	Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios.	
Procedimientos Específicos	P1	Comprobar que las consideraciones dadas a la seguridad e implicaciones de seguridad de interconectar dichas instalaciones incluyan: a) vulnerabilidades conocidas en los sistemas de administración y contabilidad donde la información es compartida por diferentes partes de la organización. b) vulnerabilidades de información en sistemas de comunicación de negocios, como el grabado de llamadas telefónicas o de conferencia, las llamadas confidenciales, el almacenamiento de faxes, el correo abierto, la distribución de correo. c) políticas y controles apropiados para manejar información compartida. d) excluir categorías de información de negocios sensible y clasificar documentos si los sistemas no proveen un nivel apropiado de protección (véase el inciso 7.2). e) acceso restringido a la información diaria relacionado con individuos selectos, como el personal que trabaja en proyectos sensibles. f) categorías de personal, contratistas o socios de negocios a los que se les permite el uso del sistema y de las locaciones desde donde puede ser accesado (véase 6.2 y 6.3). g) instalaciones restringidas seleccionadas para categorías de usuario especificas. h) identificación del estado de usuarios, como los empleados de la organización o contratistas en los directorios para beneficio de otros usuarios. i) retención y soporte de la información colgada en el sistema (véase el inciso 10.5.1). j) requisitos en el retraso y en los arreglos (véase capitulo 14).
Documentos por revisar	D1	Documento de seguridad para sistemas de información de negocios
	D2	Documento de interconexión entre sistemas de información de negocios

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.9.**	**Servicios de comercio electrónico**
Control	**10.9.1.**	**Comercio Electrónico**
Objetivo	La información envuelta en el comercio electrónico pasando a través de redes públicas, deben ser protegidas de actividad fraudulenta, disputas de contratos y de acceso y modificación no autorizada.	
Procedimientos Específicos	P1	Constatar que las consideraciones de seguridad para el comercio electrónico incluye lo siguiente: a) el nivel de confidencia que cada parte requiere en la identidad demanda. b) los procesos de autorización asociados con el que puede designar los precios, ediciones o firmas en los documentos de negocio. c) asegurar que los socios de negocio se encuentran totalmente informados de sus autorizaciones. d) determinar los requerimientos de confidencialidad, integridad, prueba de despacho y recepción de los documentos clave y la no negación de contratos, como por ejemplo los que están asociados con los procesos de ofrecimiento y contrato. e) el nivel de confianza requerido en la integridad de las listas de precio anunciadas. f) la confidencialidad de cualquier dato o información sensible, g) la confidencialidad e integridad de cualquier orden de transacción, información de pago, detalles de direcciones de entrega y confirmaciones de recibos. h) el grado de verificación apropiado para verificar la información de pago suministrada por un cliente. i) selección de la forma de establecimiento de pago más apropiada con el fin de evitar fraudes. j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de orden. k) evitar la pérdida o duplicidad de la información de transacciones. l) confiabilidad asociada con cualquier transacción fraudulenta. m) requisitos de seguro.
Documentos por revisar	D1	Documento especificación del servicio de comercio electrónico.
	D2	Política de seguridad de comercio electrónico

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.9.**	**Servicios de comercio electrónico**
Control	**10.9.2.**	**Transacciones en línea**
Objetivo	La información implicada en las transacciones en línea debe ser protegida para prevenir la transmisión incompleta, ruta equivocada, alteración no autorizada de mensajes, acceso no autorizado, duplicado no autorizado del mensaje o reproducción.	
Procedimientos Específicos	P1	Verificar que las consideraciones de seguridad para las transacciones en línea incluyen lo siguiente: a) el uso de firmas electrónicas por cada una de las partes envueltas en la transacción. b) los medios de comunicación entre todas las partes implicadas deben ser cifrados. c) todos los aspectos de la transacción, asegurando que: 1) las credenciales de usuario de todas las partes son validas y verificadas 2) la transacción quede confidencial 3) la privacidad asociada con todas las partes es retenida. d) los protocolos utilizados para comunicarse entre todas las partes debe ser seguro. e) asegurar que el almacenamiento de los detalles de la transacción estén localizados fuera de cualquier ambiente público, como en un plataforma de almacenamiento existente en el Intranet de la organización, y que no sea retenida ni expuesta en un medio de almacenamiento al que se puede acceder por Internet. f) cuando una autoridad confiable sea usada (para propósitos de publicar o mantener firmas digitales y/o certificados digitales) la seguridad es integrada a través de todo proceso de gestión del certificado/firma.
Documentos por revisar	D1	Documento de seguridad para transacciones en línea
	-	-

Dominio	**10.**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**
Categoría	**10.9.**	**Servicios de comercio electrónico**
Control	**10.9.3.**	**Información pública disponible**
Objetivo	La integridad de la información que se ha hecho disponible en un sistema público debe ser protegido para prevenir modificaciones no autorizadas.	
Procedimientos Específicos	P1	Verificar que los sistemas de publicación electrónicos son controlados cuidadosamente, especialmente los que permiten retroalimentación e ingreso directo de la información, con el fin que: a) la información obtenida concuerde con cualquier legislación de protección de datos (véase el inciso 15.1.4). b) el ingreso y procesamiento de información en el sistema será procesado completamente y actualizado a tiempo. c) la información sensible será protegida durante la recolección, procesamiento y almacenamiento. d) el acceso al sistema público no permite el ingreso involuntario a redes a las que el sistema se encuentre conectado.
	P2	**Proceso formal aprobado** Verificar que exista un proceso formal aprobado antes de que la información esté públicamente disponible. Es decir, todos los ingresos provistos desde el exterior al sistema son verificados y aprobados.
Documentos por revisar	D1	Políticas de seguridad sobre disponibilidad de información pública
	D2	Documentos de procesos formales para la publicación de información

4.7. DOMINIO 11: Control de accesos#

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.1**	**Requisitos de negocio para el control de acceso.**
Control	**11.1.1.**	**Política de control de accesos.**
Objetivo	Establecer, documentar y revisar una política de control de acceso basada en los requerimientos de seguridad y del negocio.	
Procedimientos Específicos	P1	**Política de accesos.** Verificar que las reglas y los derechos de cada usuario o grupo de usuarios se establezcan claramente en una política de acceso y contemplar lo siguiente: a) requisitos de seguridad de cada aplicación de negocio individualmente. b) identificación de toda la información relativa a las aplicaciones y los riesgos que la información esta enfrentando. c) políticas para la distribución de la información y las autorizaciones (por ejemplo, el principio de suministro sólo de la información que se necesita conocer y los niveles de seguridad para la clasificación de dicha información) (véase el inciso 7.2). d) coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes. e) legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios (véase el inciso 15.1). f) perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos. g) administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión. h) segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos. i) requerimientos para la autorización formal de los pedidos de acceso (véase el inciso 11.2.1). j) requerimientos para la revisión periódica de los controles de acceso (véase el inciso 11.2.4). k) retiro de los derechos de acceso (véase el inciso 8.3.3).
	P2	**Controles de accesos.** Comprobar que los controles de accesos son lógicos y físicos (véase 9.) y éstos deben ser considerados juntos.
	P3	**Especificaciones a usuarios y proveedores** Constatar que se dé a los usuarios y proveedores de servicios una especificación clara de los requisitos de negocio cubiertos por los controles de accesos.
	P4	**Consideraciones en controles de accesos.**

		Comprobar que se consideró para la reglas de controles de accesos lo siguiente: a) la distinción entre reglas a cumplir siempre y reglas opcionales o condicionales. b) el establecimiento de las reglas basándose en la premisa “está prohibido todo lo que no esté permitido explícitamente”, premisa que es contraria a la regla “está permitido todo lo que no esté prohibido explícitamente”, considerada más débil o más permisiva. c) los cambios en las etiquetas de información (véase 7.2.) iniciadas automáticamente por los recursos del tratamiento de la información y las que inicia el usuario manualmente. d) los cambios en las autorizaciones al usuario realizados automáticamente por el sistema de información y los que realiza un administrador. e) la distinción entre reglas que requieren o no la aprobación del administrador o de otra autoridad antes de su promulgación.
Documentos por revisar	D1	Documento de Política de Acceso.
	D2	Registro de difusión de políticas.
	D3	Documento de requerimientos de seguridad de la organización
	D4	Documento de requerimientos del negocio de la organización

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.2.**	**Gestión de acceso de usuarios**
Control	**11.2.1.**	**Registro de usuarios**
Objetivo	Formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.	
Procedimientos Específicos	P1	**Identificador único** Verificar la utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debería permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados.
	P2	**Comprobación de autorización** Verificar que el propietario del servicio compruebe la autorización del usuario para utilizar el sistema o el servicio de información. También aprobación de la gerencia.
	P3	**Nivel de acceso asignado** Verificación de la adecuación del nivel de acceso asignado al propósito del negocio (véase el inciso 11.1) y su consistencia con la política de seguridad de la organización (por ejemplo, su no contradicción con el principio de segregación de tareas (véase el inciso10.1.3).
	P4	**Entrega de derechos de acceso a usuarios** Constatar, mediante firma, la entrega a los usuarios de una relación escrita de sus derechos de acceso
	P5	**Provisión de acceso al servicio** Verificar la garantía de que no se provee acceso al servicio hasta que se haya completado los procedimientos de autorización.
	P6	**Mantenimiento de registro.** Constatar el mantenimiento de un registro formalizado de todos los autorizados para usar el servicio y la eliminación inmediata de las mismas cuando el usuario deja la organización cambien de trabajo en ella.
	P7	**Cuentas de usuario e identificadores redundantes.** Comprobar la revisión periódica y eliminación de identificadores y cuentas de usuario redundantes.
	P8	**Asignación a identificadores redundantes.** Verificar garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.
Documentos por revisar	D1	Contratos laborales y de servicio
	D2	Documento de requisitos de negocio de la organización
	D3	Procedimiento de registro de altas y bajas de usuarios.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.2.**	**Gestión de acceso de usuarios**
Control	**11.2.2.**	**Gestión de privilegios**
Objetivo	Restringir y controlar el uso y asignación de privilegios.	
Procedimientos Específicos	P1	**Privilegios asociados a cada elemento del sistema** Verificar la identificación de los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación; así como las categorías de empleados que necesitan de ellos.
	P2	**Asignación de privilegios** Verificar que se asignan privilegios a los individuos según los principios de "necesidad de su uso" y "caso por caso" y en línea con la política de control de acceso (véase 11.1.1.), por ejemplo, el requisito mínimo para cumplir su función sólo cuando se necesite.
	P3	**Proceso de autorización y Registro de todos los privilegios asignados** Constatar el mantenimiento de un proceso de autorización y un registro de todos los privilegios asignados. Que no se otorgan privilegios hasta que el proceso de autorización ha concluido.
	P4	**Desarrollo y uso de rutinas del sistema** Comprobar la promoción del desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios.
	P5	**Desarrollo y uso de programas sin privilegios** Comprobar la promoción del desarrollo y uso de programas que evitan la necesidad de correr con privilegios.
	P6	**Distinción de identificador para privilegios.** Constatar que se asignan los privilegios a un identificador de usuario distinto al asignado para un uso normal.
Documentos por revisar	D1	Registro de privilegios asignados.
	D2	Documento de privilegios disponibles para asignar.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.2.**	**Gestión de acceso de usuarios**
Control	**11.2.3.**	**Gestión de contraseñas de usuario.**
Objetivo	Controlar la asignación de contraseñas por medio de un proceso de gestión formal.	
Procedimientos Específicos	P1	**Compromiso de mantener contraseñas en secreto.** Constatar que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo (compromiso que podría incluirse en los términos y condiciones del contrato de empleo, véase el inciso 8.1.3).
	P2	**Contraseña temporal inicial.** Comprobar que inicialmente se proporcione una contraseña temporal segura (véase 11.3.1.) que forzosamente se deba cambiar inmediatamente después.
	P3	**Verificar identidad de un usuario para realizar cambios de contraseña.** Verificar que se establecieron procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de remplazo o temporal.
	P4	**Conducto seguro de envío de contraseñas temporales a usuarios.** Verificar que se establecieron conductos seguros para hacer llegar las contraseñas temporales a los usuarios. Se debería evitar su envío por terceros o por mensajes no cifrados de correo electrónico.
	P5	**Contraseñas temporales únicas y no obvias.** Verificar que las contraseñas temporales sean únicas para cada individuo y no ser obvias.
	P6	**Acuse de recibido de contraseñas.** Verificar que usuarios remitan acuse de recibo de contraseñas.
	P7	**Protección de contraseñas guardadas.** Comprobar que las contraseñas nunca sean almacenadas en sistemas de cómputo sin ser protegidas.
	P8	**Contraseñas por defecto.** Comprobar que las contraseñas por defecto de los vendedores sean alteradas después de la instalación de los sistemas o software.
Documentos por revisar	D1	Compromisos de usuarios a mantener en secreto las contraseñas.
	D2	Registros de falsos negativos y falsos positivos.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.2.**	**Gestión de acceso de usuarios**
Control	**11.2.4.**	**Revisión de los derechos de acceso de los usuarios.**
Objetivo	Establecer, por parte de gerencia, un proceso formal de revisión periódica de los derechos de acceso de los usuarios.	
Procedimientos Específicos	P1	**Derechos de acceso** Verificar la revisión de los derechos de acceso de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses) y después de cualquier cambio como promoción, degradación o término del empleo (véase el inciso 11.2.1), traslado desde un empleo a otro dentro de la misma organización.
	P2	**Accesos con privilegios** Comprobar la revisión de las autorizaciones de derechos de acceso con privilegios especiales (véase 11.2.2.), y su registro.
Documentos por revisar	D1	Registro de cambios en cuentas privilegiadas.
	D2	Derechos de accesos de los usuarios.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.3.**	**Responsabilidades de los usuarios.**
Control	**11.3.1.**	**Uso de contraseñas.**
Objetivo	Los usuarios sigan buenas prácticas de seguridad para la selección y uso de sus contraseñas.	
Procedimientos Específicos	P1	**Usuarios informados.** Verificar que todos los usuarios estén informados acerca de: a) mantener la confidencialidad de las contraseñas. b) evitar guardar registros (papel, archivos de software o dispositivos) de las contraseñas, salvo si existe una forma segura de hacerlo y el método de almacenamiento ha sido aprobado. c) cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema. d) seleccionar contraseñas de buena calidad, con una longitud mínima caracteres, que sean: 1) fáciles de recordar. 2) no estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario, por ejemplo, nombres, fechas de nacimiento, números de teléfono, etc.. 3) no sean vulnerables a ataques de diccionario (no consisten en palabras incluidas en diccionarios). 4) estén carentes de caracteres consecutivos repetidos o que sean todos números o todas letras. e) cambiar las contraseñas a intervalos de tiempo regulares o en proporción al número de accesos (las contraseñas de las cuentas con privilegios especiales deberían cambiarse con más frecuencia que las normales), evitando utilizar contraseñas antiguas o cíclicas. f) cambiar las contraseñas temporales asignadas para inicio, la primera vez que se ingrese al sistema. g) no incluir contraseñas en ningún procedimiento automático de conexión, que, las deje almacenadas permanentemente. h) no compartir contraseñas de usuario individuales. i) no utilizar la misma contraseña para propósitos personales o de negocio.
	P2	**Pérdida u olvido de contraseña** Comprobar que la gestión de los sistemas de ayuda que tratan con problemas de pérdida u olvido de contraseña tenga un cuidado especial ya que esto también significa medios de ataque al sistema de contraseñas.
Documentos por revisar	D1	Procedimientos en caso de pérdida u olvido de contraseña.
	-	-

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.3.**	**Responsabilidades de los usuarios.**
Control	**11.3.2.**	**Equipo informático de usuario desatendido**
Objetivo	Los usuarios aseguran que los equipos informáticos desatendidos estén debidamente protegidos.	
Procedimientos Específicos	P1	**Conocimiento de requisitos de seguridad y sus procedimientos.** Verificar que todos los usuarios y proveedores de servicios conocen los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos, así como sus responsabilidades para implantar dicha protección.
	P2	**Buenas prácticas para proteger equipos informáticos desatendidos.** Verificar que se recomiende: a) cancelar todas las sesiones activas antes de marcharse, salvo si se dispone de una herramienta de bloqueo general, por ejemplo, una contraseña para protector de pantalla. b) desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión (y no sólo apagar el terminal o el computador personal). c) proteger el terminal o el puesto de trabajo cuando no estén en uso con un bloqueador de teclado o una medida similar, por ejemplo, una contraseña de acceso (véase el inciso 11.3.3).
Documentos por revisar	D1	Requisitos de seguridad
	D2	Contratos con empleados y proveedores.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.3.**	**Responsabilidades de los usuarios.**
Control	**11.3.3.**	**Política de pantalla y escritorio limpio.**
Objetivo	Adoptar una política de escritorio limpio para papeles y medios removibles de almacenamiento así como una política de pantalla limpia para instalaciones de procesamiento de información.	
Procedimientos Específicos	P1	**Consideraciones para la política** Verificar que se haya realizado la clasificación de la información (véase 7.2.), revisado los requerimientos legales y contractuales (véase 15.1.), los riesgos correspondientes y los aspectos culturales de la organización.
	P2	**Asegurar información crítica y sensible.** Comprobar que la información crítica y sensible del negocio (papel o medios electrónicos) esté asegurada (seria ideal un caja fuerte, gavetas u otras formas de muebles de seguridad) cuando no sea requerido, especialmente cuando la oficina este vacía.
	P3	**Computadores, terminales y puntos salientes protegidos.** Verificar que los computadores y terminales estén apagados o protegidos con un mecanismo de protección de pantalla o de teclado controlado por contraseña u otro mecanismo de autentificación, cuando éstas se encuentren desatendidos y deben ser protegidas por cerraduras clave, contraseñas u otro tipo de control cuando no sean utilizados. Verificar que los puntos salientes o entrantes de correo y los faxes desatendidos estén protegidos.
	P4	**Remover documentos de las impresoras de inmediato** Verificar que los documentos que contienen información sensible y clasificada sean removidos de las impresoras de inmediato.
	P5	**Uso no autorizado de tecnologías de reproducción** Constatar que se prevenga el uso no autorizado de fotocopiadoras y otras tecnologías de reproducción como scanner o cámaras digitales.
Documentos por revisar	D1	Documento de política de pantalla y escritorio limpio.
	D2	Registro de protección a computadores, terminales y puntos salientes.
	D3	Registro de uso de tecnologías de reproducción.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.1.**	**Política de uso de los servicios de la red**
Objetivo	Los usuarios sólo deberían tener acceso directo a los servicios para los que estén autorizados de una forma específica.	
Procedimientos Específicos	P1	**Política de uso de las redes y servicios de red** Verificar que se formule la política de uso de las redes y los servicios de la red que es conveniente que cubre: a) las redes y los servicios de la red a los que se puede acceder. b) los procedimientos de autorización para determinar quién puede acceder a qué redes y a qué servicios de la red. c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de las redes y a los servicios de la red. d) los medios usados para el acceso y los servicios de red (las condiciones para permitir el acceso por discado al proveedor de servicio de Internet o a un sistema remoto).
	P2	**Coherencia de la política** Comprobar que la política sea coherente con la política de control de accesos de la organización (véase 11.1.)
Documentos por revisar	D1	Política de control de accesos.
	D2	Política de uso de los servicios de la red

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.2.**	**Autentificación de usuario para conexiones externas**
Objetivo	Utilizar métodos apropiados de autentificación para controlar el acceso de usuarios remotos.	
Procedimientos Específicos	P1	**Autentificación de usuarios remoto** Comprobar que la autentificación de usuarios remoto se realiza utilizando, por ejemplo, una técnica basada en criptografía, símbolos de hardware o un protocolo de desafío/respuesta. También utilizando líneas privadas dedicadas, con el fin de proveer aseguramiento en la fuente de conexiones.
	P2	**Control adicional para redes inalámbricas** Verificar la autenticación implementada para el control de acceso de redes inalámbricas.
Documentos por revisar	D1	Documentación de técnicas utilizadas para la autenticación de usuarios.
	-	-

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.3.**	**Identificación de equipos en las redes**
Objetivo	Considerar las identificaciones automáticas de equipos como medios para autentificar conexiones desde locales y equipos específicos.	
Procedimientos Específicos	P1	**Identificador dentro o adjunto al equipo** Verificar la existencia de un identificador dentro o adjunto al equipo para indicar si el equipo está autorizado para conectarse a la red.
	P2	**Protección física** Constatar la necesidad de considerar protección física del equipo con el fin de mantener la seguridad de los identificadores del equipo
Documentos por revisar	D1	Documento de relación identificador-red para autorización a conexión.
	D2	Lista de identificadores de equipos

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.4.**	**Diagnóstico remoto y configuración de protección de puertos**
Objetivo	Controlar el acceso físico y logístico para diagnosticar y configurar puertos.	
Procedimientos Específicos	P1	**Controles de acceso físico al puerto** Comprobar la existencia de controles potenciales para el acceso de diagnóstico y configuración de puertos como el uso de cierre con llave y de procedimientos para controlar el acceso físico al puerto
	P2	**No requerimientos para funcionalidad del negocio** Verificar que los puertos, servicios e instalaciones similares instaladas en una computadora o instalación de computo que no son requeridas específicamente para la funcionalidad del negocio, estén inhabilitados o sean removidos.
Documentos por revisar	D1	Requerimientos de funcionalidad del negocio de la organización
	D2	Procedimientos de apoyo para controlar el acceso físico al puerto.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.5.**	**Segregación en las redes**
Objetivo	Segregar los grupos de servicios de información, usuarios y sistemas en las redes.	
Procedimientos Específicos	P1	**Métodos para controlar la seguridad de grandes redes.** Comprobar la existencia de métodos para controlar la seguridad en redes grandes.
	P2	**Evaluación de riesgos en cada dominio de red.** Verificar que los dominios sean definidos basados en una evaluación de riesgos y los diferentes requisitos de seguridad entre cada uno de los dominios.
	P3	**Implantar un gateway seguro entre dos redes.** Configuración del gateway que filtre el tráfico entre las redes (véase 11.4.6 y 11.4.7.) y bloquee los accesos no autorizados de acuerdo con la política de control de accesos de la organización (véase 11.1.)
	P4	**Lineamiento de los criterios de segregación en dominios con política de control de accesos** Comprobar que los criterios para segregar las redes en dominios se basen en la política de control de accesos y en los requisitos de acceso (véase 10.1.) teniendo en cuenta el costo relativo y el impacto en el rendimiento por la incorporación de la tecnología adecuada de enrutamiento de gateway en la red (véanse 11.4.6. y 11.4.7.)
	P5	**Criterios basados en el valor y clasificación de la información almacenada o procesada en la red.** Verificar que la segregación de redes en dominios esté basada en el valor y clasificación de la información almacenada o procesada en la red, niveles de confianza o líneas de negocio.
	P6	**Redes inalámbricas desde una red interna hacia una privada.** Verificar que se llevó a cabo una evaluación de riesgos para identificar controles (una fuerte autentificación, métodos criptográficos y frecuencia de selección) para mantener una segregación de red.
Documentos por revisar	D1	Documento de criterios para segregación de redes
	D2	Política de control de accesos y requisitos de accesos.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.6.**	**Control de conexión a las redes**
Objetivo	Basar los requisitos de la política de control de accesos para redes compartidas en los requisitos de las aplicaciones del negocio (véase el inciso 11.1).	
Procedimientos Específicos	P1	**Mantenimiento de los derechos de acceso de los usuarios.** Los derechos de acceso de los usuarios deben ser mantenidos y actualizados como requiere la política de control de accesos (véase el inciso 11.1.1).
	P2	**Capacidad de restricción** Verificar que la capacidad de conexión de los usuarios son restringidas a través de entradas que filtren el trafico por medio de tablas o reglas pre definidas, como por ejemplo: a) correo electrónico. b) transferencia de archivos. c) acceso interactivo. d) acceso a la aplicación.
Documentos por revisar	D1	Política de control de accesos y requisitos de accesos.
	D2	Tablas o reglas para filtros de conexión de usuarios.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.4.**	**Control de acceso a la red**
Control	**11.4.7.**	**Control de enrutamiento en la red**
Objetivo	Implementar controles de enrutamiento que garanticen que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso a las aplicaciones.	
Procedimientos Específicos	P1	**Mecanismos para validar fuente y destino de los mensajes.** Verificar que la implementación de los mecanismos para validar la fuente y los destinos de los mensajes en puntos de control de redes internas o externas, tuvo en cuenta la robustez de los mismos.
	P2	**Lineamiento con la política de control de accesos** Verificar que los requisitos para los controles de enrutamiento están basados en la política de control de accesos (véase 11.1.)
Documentos por revisar	D1	Controles de enrutamiento
	D2	Política de control de accesos a aplicaciones

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.1.**	**Procedimientos de conexión de terminales**
Objetivo	El acceso a los servicios de información debería estar disponible mediante un proceso de conexión seguro.	
Procedimientos Específicos	P1	**Información del sistema en proceso de conexión.** Verificar que se diseñó un procedimiento para conectarse al sistema informático que minimiza la posibilidad de accesos no autorizados. El proceso de conexión muestra el mínimo posible de información sobre el sistema para no facilitar ayuda innecesaria a usuarios no autorizados. a) no mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión. b) mostrar un mensaje que advierta la restricción de acceso al sistema sólo a usuarios autorizados. c) no ofrecer mensajes de ayuda durante el proceso de conexión que puedan guiar a usuarios no autorizados. d) validar la información de conexión sólo tras rellenar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicar qué parte de esos datos es correcta o no. e) limitar el número de intentos fallidos de conexión (se recomienda tres) y considerar: 1) el registro de los intentos fallidos de conexión. 2) un tiempo forzoso de espera antes de permitir un nuevo intento de conexión o su rechazo sin una autorización específica. 3) la desconexión de la comunicación de datos. 4) el envío de un mensaje de alerta a la consola del sistema si se alcanza el número máximo de oportunidades de conexión. 5) establecer el número de pruebas de contraseña en conjunción con su largo mínimo y el valor de los sistemas que están siendo protegidos. f) limitar los tiempos máximo y mínimo permitidos para efectuar el proceso de conexión. g) mostrar la siguiente información tras completar una conexión con éxito: 1) fecha y hora de la anterior conexión realizada con éxito. 2) información de los intentos fallidos desde la última conexión realizada con éxito. h) no mostrar la contraseña que se ingresa o considerar esconderla con caracteres simbólicos. i) no transmitir contraseñas en texto legible a través de la red.
	P2	**Transmisión de contraseñas** Verificar que las contraseñas no sean transmitidas en texto legible durante la sesión de conexión, pues pueden ser capturadas por programas "succionadores" de red.
Documentos por revisar	D1	Documento de diseño e implementación del módulo de acceso al sistema
	D2	Documento de diseño e implantación del módulo de acceso al sistema

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.2.**	**Identificación y autenticación del usuario**
Objetivo	Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autentificación adecuada para verificar la identidad de estos.	
Procedimientos Específicos	P1	**Controles para el universo de usuarios.** Verificar que el control es aplicado para todos los tipos de usuario (incluido administradores de red y de base de datos, los programadores de sistemas y el personal técnico de apoyo).
	P2	**Cuentas privilegiadas** Verificar que las actividades regulares del usuario no sean realizadas desde cuentas privilegiadas.
Procedimientos Específicos	P3	**IDs genéricos** Comprobar que los ID's genéricos utilizados por individuos solo son permitidos donde las funciones o acciones llevadas a cabo no requieren ser trazadas (como la lectura) o cuando existan otros controles establecidos (contraseñas genéricas utilizadas solamente por un grupo de personas a la vez y conectándose en dicho momento).
	P4	**Requerimiento de fuerte autentificación e identificación** Constatar la utilización de métodos alternativos a las contraseñas como medios criptográficos, tarjetas inteligentes o medios biométricos.
Documentos por revisar	D1	Documento de trazabilidad de IDs con empleados
	D2	Registro de cuentas privilegiadas
	D3	Log de los sistemas
	D4	Documento de controles de seguridad

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.3.**	**Sistema de Gestión de contraseñas**
Objetivo	Los sistemas de gestión de contraseñas deberían proporcionar un medio eficaz e interactivo para asegurar la calidad de las mismas	
Procedimientos Específicos	P1	Verificar que se impone el uso de contraseñas individuales
	P2	Verificar que se permite que los usuarios escojan sus contraseñas, las cambien e incluyan un procedimiento de confirmación para evitar errores al introducirlas
	P3	Comprobar que se impone la selección de contraseñas de calidad
	P4	Comprobar que se exige el cambio de contraseñas
	P5	Comprobar la exigencia del cambio de contraseñas iniciales en la primera conexión (véase 11.2.3.)
	P6	Verificar que se mantiene un registro de las anteriores contraseñas utilizadas e impedir su reutilización
	P7	Constatar que no se muestran las contraseñas en la pantalla cuando se están introduciendo
	P8	Verificar que se almacenan las contraseñas y datos del sistema de aplicaciones en sitios distintos
	P9	Verificar que se almacenan las contraseñas en forma cifrada mediante un algoritmo de cifrado unidireccional
Documentos por revisar	D1	Documento de análisis y diseño del sistema de gestión de contraseñas
	D2	Documento de procedimientos para la administración de contraseñas del usuario.
	D3	Documento de procedimientos de seguridad de contraseñas

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.4.**	**Utilización de las facilidades del sistema**
Objetivo	La mayoría de las instalaciones informáticas disponen de programas del sistema capaces de eludir las medidas de control del sistema o de las aplicaciones. Es fundamental que su uso se restrinja y se mantenga fuertemente controlado	
Procedimientos Específicos	P1	Comprobar el uso de procedimientos de autenticación, identificación y autorización para las facilidades del sistema
	P2	Verificar que se separan las facilidades del sistema de las aplicaciones de software.
	P3	Constatar que se limitan el uso de las facilidades del sistema al mínimo número de usuarios autorizados y fiables (véase también 11.2.2).
	P4	Verificar que se autoriza el uso de las facilidades con un propósito concreto (ad hoc).
	P5	Verificar que se limita la disponibilidad de las facilidades del sistema, por ejemplo, durante un cambio autorizado.
	P6	Comprobar que se registra (logging) todo uso de las facilidades del sistema.
	P7	Verificar que se define y documenta los niveles de autorización para las facilidades del sistema.
	P8	Comprobar que se desactiva o retira todas las facilidades basadas en software y el software de sistemas que no sean necesarios.
	P9	Verificar que no se pone en disponibilidad las facilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas donde la segregación de tareas sea requerida.
Documentos por revisar	D1	Procedimientos de autenticación, identificación y autorización para facilidades del sistema
	D2	Documento de especificaciones de facilidades del sistema
	D3	Documento de niveles de autorización para facilidades del sistema

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.5.**	**Desconexión automática de sesiones**
Objetivo	Las sesiones se deberían desactivar tras un periodo definido de inactividad.	
Procedimientos Específicos	P1	Comprobar que se borra la pantalla y se cierra la aplicación y las sesiones de conexión a red tras un periodo definido de inactividad.
	P2	Verificar que el tiempo de desactivación refleje los riesgos de seguridad del área, la clasificación de la información que se maneja, las aplicaciones que se utilizan y los riesgos relacionados con los usuarios de los equipos.
Documentos por revisar	D1	Documento de análisis de riesgos de seguridad.
	D2	Documento de clasificación de la información.

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.5.**	**Control de acceso al sistema operativo**
Control	**11.5.6.**	**Limitación del tiempo de conexión**
Objetivo	Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.	
Procedimientos Específicos	P1	**Uso de aplicaciones sensibles** Verificar el uso de aplicaciones sensibles, en especial para terminales instalados en áreas de alto riesgo, las públicas o no cubiertas por la gestión de seguridad de la organización. Restricciones como por ejemplo: a) el uso de 'ventanas' de tiempo predeterminadas, por ejemplo para transmisiones de archivos en batch, o para sesiones interactivas regulares de corta duración. b) la restricción de tiempos de conexión al horario normal de oficina, si no existen requisitos para operar fuera de este horario. c) considerar la re-autentificación en intervalos medidos.
Documentos por revisar	-	-
	-	-

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.6.**	**Control de acceso a las aplicaciones y la información**
Control	**11.6.1.**	**Restricción de acceso a la información**
Objetivo	Las restricciones en los tiempos de conexión ofrecen seguridad adicional para aplicaciones de alto riesgo.	
Procedimientos Específicos	P1	Verificar que se establecen menús para controlar los accesos a las funciones del sistema de aplicaciones.
	P2	Comprobar que se controlar los derechos de accesos de los usuarios, por ejemplo lectura, escritura, borrado, ejecución.
	P3	Comprobar que se controlan los derechos de acceso de otras aplicaciones
	P4	Verificar que se aseguran que las salidas de los sistemas de aplicación que procesan información sensible, sólo contienen la información correspondiente para el uso de la salida y se envían, únicamente, a los terminales y sitios autorizados, incluyendo la revisión periódica de dichas salidas para garantizar la supresión de información redundante.
Documentos por revisar	D1	Documentos de controles para derechos de accesos externos.
	-	-

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.6.**	**Control de acceso a las aplicaciones y la información**
Control	**11.6.2.**	**Aislamiento de sistemas sensibles**
Objetivo	Los sistemas sensibles pueden necesitar entornos informáticos dedicados (aislados).	
Procedimientos Específicos	P1	Comprobar que el propietario indicó explícitamente y documentar la "sensibilidad" de ésta (véase 7.1.2.)
	P2	Constatar que cuando una aplicación sensible se ejecute en un entorno compartido, se identifican y acuerdan con su propietario los sistemas de aplicación con los que compartan recursos.
Documentos por revisar	D1	Documento de sensibilidad de las aplicaciones.
	D2	Documento de recursos compartidos entre sistemas

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.7.**	**Informática móvil y teletrabajo**
Control	**11.7.1.**	**Informática móvil y comunicaciones**
Objetivo	Adoptar una política formal y medidas de seguridad apropiadas con el fin de protegernos contra los riesgos cuando se usan dispositivos de informática.	
Procedimientos Específicos	P1	**Uso** Verificar que se tiene un especial cuidado para asegurar que la información de negocio no se comprometa cuando se usan dispositivos de informática móvil como portátiles, agendas, calculadoras y teléfonos móviles.
	P2	**Riesgos** Constatar que se formalizó una política que tenga en cuenta los riesgos de trabajar con dispositivos de informática móvil, especialmente en entornos desprotegidos.
	P3	**Protección** Verificar la instalación de una protección para dispositivos de informática móvil en lugares públicos, salas de reuniones y otras áreas desprotegidas fuera de locales de la organización.
	P4	**Software malicioso** Verificar la instalación y actualización de procedimientos contra el software malicioso (véase 10.4.)
	P5	**Backups** Constatar la realización regular de backups de información crítica de negocio con sus respectivas protecciones contra hurto o pérdida de información.
	P6	**Protección física** Comprobar la protección física de los dispositivos de informática móvil contra el robo.
Documentos por revisar	D1	Procedimientos de protección física de dispositivos de informática móvil.
	D2	Análisis de riesgo de dispositivos de informática móvil
	D3	Política de seguridad de informática móvil

Dominio	**11.**	**CONTROL DE ACCESOS**
Categoría	**11.7.**	**Informática móvil y teletrabajo**
Control	**11.7.2.**	**Teletrabajo**
Objetivo	Se deberían desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.	
Procedimientos Específicos	P1	**Autorización** Constatar que las organizaciones solo autorizan las actividades de teletrabajo si han satisfecho las disposiciones y controles de seguridad apropiados y cumple la política de seguridad de la organización
	P2	**Acuerdos adecuados** Verificar que se consideró lo siguiente para que existan acuerdos adecuado para este tipo de trabajo: a) la seguridad física real del lugar de teletrabajo, teniendo en cuenta la del edificio y la de su entorno local. b) el entorno de teletrabajo propuesto. c) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la criticidad de la información a acceder y el paso por alto del enlace de comunicación y de la criticidad del sistema interno. d) la amenaza de acceso no autorizado a información y recursos por otras personas próximas, por ejemplo, la familia o amigos. e) el uso de redes de casa y los requisitos o restricciones de la configuración de los servicios inalámbricos. f) las políticas y procedimientos para prevenir las disputas concernientes a los derechos de la propiedad intelectual desarrollada en equipos privados propios. g) el acceso a un equipo privado propio (para verificar la seguridad de la maquina o durante una investigación), que puede ser prevenido por la legislación. h) los acuerdos de licencia de software que hará que dichas organizaciones se vuelvan confiables para el licenciamiento de software de clientes en las estaciones de trabajo pertenecientes a empleados, contratistas o terceros. i) la protección antivirus y los requerimientos de firewall.
	P3	**Controles y adecuaciones** Verificar la instalación de una protección para dispositivos de informática móvil en lugares públicos, salas de reuniones y otras áreas desprotegidas fuera de locales de la organización. a) el aprovisionamiento del equipo y mobiliario adecuados para las actividades de teletrabajo, donde no esta permitido el uso de equipos privados propios que no estén bajo el control de la organización. b) la definición del trabajo permitido, las horas de trabajo, la clasificación de la información que puede utilizar y los sistemas y servicios internos a los que el tele-trabajador esté autorizado a acceder.

		c) el suministro del equipo de comunicación adecuado, incluidos los métodos para asegurar el acceso remoto d) la seguridad física. e) reglas y guías sobre la familia y el acceso de visitas al equipo y la información. f) proporcionar el soporte y mantenimiento para el hardware y el software. g) proporcionar una póliza de seguros. h) los procedimientos de respaldo y continuidad del negocio. i) la auditoria y seguimiento de la seguridad. j) la revocación de autorizaciones, derechos de acceso y devolución del equipo cuando cesen las actividades de teletrabajo.
	P4	**Software malicioso** Verificar la instalación y actualización de procedimientos contra el software malicioso (véase 10.4.)
	P5	**Backups** Constatar la realización regular de backups de información crítica de negocio con sus respectivas protecciones contra hurto o pérdida de información.
	P6	**Protección física** Comprobar la protección física de los dispositivos de informática móvil contra el robo.
Documentos por revisar	D1	Procedimientos de protección física de dispositivos de informática móvil.
	D2	Análisis de riesgo de dispositivos de informática móvil
	D3	Política de seguridad de informática móvil

4.8. DOMINIO 12: Adquisición, desarrollo y mantenimiento de sistemas

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.1.**	**Requisitos de seguridad de los sistemas**
Control	**12.1.1.**	**Análisis y especificación de los requisitos de seguridad**
Objetivo	Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control.	
Procedimientos Específicos	P1	**Consideraciones para los requisitos de seguridad** Comprobar que se consideren los controles automatizados a ser incorporados en el sistema y la necesidad de controles manuales de apoyo. Se aplican consideraciones similares cuando se evalúen, desarrollen o compren paquetes de software para aplicaciones de negocio.
	P2	**Reflejo del valor de los activos de información implicados** Verificar que los requisitos y controles de seguridad reflejen el valor de los activos de información implicados (véase el inciso 7.2) y el posible daño a la organización que resultaría de fallos o ausencia de seguridad.
	P3	**Etapas iniciales** Verificar que los requisitos del sistema para la seguridad de información y procesos para implementar la seguridad son integrados en las etapas iniciales de los proyectos de sistema de información. Los controles introducidos en la etapa de diseño son significantemente menos costos de implementar y mantener que los que se incluyen durante o después de la implementación.
	P4	**Productos comprados** Comprobar, si los productos son comprados, la realización de una prueba formal y un proceso de adquisición. Los contratos con el proveedor deben indicar los requisitos de seguridad. Si los requisitos no satisfacen la funcionalidad de la seguridad en un producto se reconsidera los riesgos introducidos y los controles asociados antes de comprar el producto. Donde se suministre una funcionalidad adicional que cause un riesgo en la seguridad, se desactiva o se revisa la estructura del control propuesto para determinar si se puede tomar ventaja de la funcionalidad disponible.
Documentos por revisar	D1	Documento de evaluación de productos de seguridad de TI
	D2	Requisitos de seguridad de la organización
	D3	Documento de valorización de activos de información

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.2.**	**Seguridad de las aplicaciones del sistema**
Control	**12.2.1.**	**Validación de los datos de entrada**
Objetivo	Validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas.	
Procedimientos Específicos	P1	**Verificaciones** Comprobar que se aplicó verificaciones a la entrada de las transacciones, de los datos de referencia (por ejemplo nombres y direcciones, límites de crédito, números de clientes) y de las tablas de parámetros (por ejemplo precios de venta, tasas de cambio de divisas, tasas de impuestos).
	P2	**Controles** Verificar que se consideró: a) entrada duplicada u otras verificaciones, como verificación de fronteras o campos limitados para especificar los rangos de los datos de entrada, para detectar los errores siguientes: 1) valores fuera de rango. 2) caracteres inválidos en los campos de datos. 3) datos que faltan o están incompletos. 4) datos que exceden los límites de volumen por exceso o defecto. 5) datos de controles no autorizados o inconsistentes. b) revisión periódica del contenido de los campos clave o los archivos de datos para confirmar su validez e integridad. c) inspección de los documentos físicos de entrada para ver si hay cambios no autorizados a los datos de entrada (todos deberían estar autorizados). d) procedimientos para responder a los errores de validación. e) procedimientos para comprobar la integridad de los datos de entrada. f) definición de las responsabilidades de todos los implicados en el proceso de entrada de datos. g) creación de un registro de actividades envueltas en el procesamiento de los datos de entrada (véase el inciso 10.10.1).
Documentos por revisar	-	-
	-	-

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.2.**	**Seguridad de las aplicaciones del sistema**
Control	**12.2.2.**	**Control del proceso interno**
Objetivo	Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados	
Procedimientos Específicos	P1	**Implantación de restricciones** Comprobar que el diseño de las aplicaciones aseguren la implantación de restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad. Áreas de riesgo específicas a considerar son: a) el uso en los programas de funciones 'añadir' y 'borrar' para cambiar los datos. b) los procedimientos para evitar programas que corran en orden equivocado o después del fallo de un proceso anterior (véase el inciso10.1.1). c) el uso de programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos. d) la protección contra ataques utilizando corridas o desbordes de buffers.
	P2	**Lista de verificación apropiada.** Verificar que existe una lista de verificación apropiada, tener las actividades documentadas y los resultados seguros.
Documentos por revisar	D1	Listas de verificación.
	D2	Documentación de actividades y resultados

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.2.**	**Seguridad de las aplicaciones del sistema**
Control	**12.2.3.**	**Integridad de mensajes**
Objetivo	Identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se deberían de identificar e implementar controles apropiados.	
Procedimientos Específicos	P1	**Identificación de incidentes frecuentes o de gran impacto** Verificar que se ha llevado a cabo una evaluación de riesgos para determinar si la integridad de los mensajes es requerida y que se ha identificado el método mas apropiado para su implementación.
Documentos por revisar	D1	Documento de implantación para autenticación
	-	-

ominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.2.**	**Seguridad de las aplicaciones del sistema**
Control	**12.2.4.**	**Validación de los datos de salida**
Objetivo	Validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias.	
Procedimientos Específicos	P1	**Admisibilidad de evidencia: si es que la evidencia puede ser utilizada en corte** Comprobar que existen validación de salidas, que incluyen: a) validaciones de verosimilitud para comprobar que los datos de salida son razonables. b) cuentas de control de conciliación para asegurar el proceso de todos los datos. c) suministro de suficiente información al lector o a un sistema de proceso subsiguiente para poder determinar la exactitud, completitud, precisión y clasificación de la información. d) procedimientos para contestar los cuestionarios de validación de salidas. e) definición de las responsabilidades de todos los implicados en el proceso de salida de datos. f) creación de un registro de actividades en el proceso de validación de los datos de salida.
Documentos por revisar	D1	Documento de validación, verificación y prueba de los sistemas y aplicaciones
	-	-

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.3.**	**Controles criptográficos**
Control	**12.3.1.**	**Política de uso de los controles criptográficos**
Objetivo	Desarrollar e implementar una política de uso de las medidas criptográficas para proteger la información.	
Procedimientos Específicos	P1	**Enfoque de gestión** Comprobar la existencia de un enfoque de gestión del uso de las medidas criptográficas a través de la organización, incluyendo los principios generales en base a los cuales se debería proteger la información del negocio (véase el inciso 5.1.1)
	P2	**Evaluación de riesgos** Verificar que la política esté basado en la evaluación de riesgos, el nivel requerido de protección es identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido.
	P3	**Uso de cifrado** Verificar el uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación
	P4	**Gestión de claves** Constatar que existe un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves.
	P5	**Roles y responsabilidades** Verificar la existencia de roles y responsabilidades de cada cual que es responsable de: 1) la implementación de la política 2) la gestión de claves, incluyendo la generación de claves (véase el inciso 12.3.2).
	P6	**Estándares adoptados** Verificar la existencia de estándares para ser adoptados en una efectiva implementación a través de la organización.
	P7	**Normas de utilización de información cifrada** Constatar la existencias de normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus)
	P8	**Controles criptográficos** Verificar que se han utilizado controles criptográficos para alcanzar diferentes objetivos de seguridad.
Documentos por revisar	D1	Documento de requisitos de seguridad de la organización
	D2	Documento de roles y responsabilidades
	D3	Procedimientos de uso de información cifrada.
	D4	Documento de Evaluación de riesgos

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.3.**	**Controles criptográficos**
Control	**12.3.2.**	**Gestión de claves**
Objetivo	La gestión de claves criptográficas debe apoyar el uso de las técnicas criptográficas en la organización.	
Procedimientos Específicos	P1	**Sistema de gestión de claves** Verificar la existencia de un sistema de gestión de claves que es un conjunto acordado de normas, procedimientos y métodos seguros para: a) generar claves para distintos sistemas criptográficos y distintas aplicaciones. b) generar y obtener certificados de clave pública. c) distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves. d) almacenar claves, incluyendo la forma de obtención de acceso a las claves por los usuarios. e) cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse. f) tratar las claves comprometidas (afectadas). g) revocar claves, incluyendo la forma de desactivarlas o retirarlas, por ejemplo, cuando tienen problemas o el usuario deja la organización (en cuyo caso las claves también se archivan). h) recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio, por ejemplo, para recuperar la información cifrada. i) archivar claves, por ejemplo, para información archivada o de respaldo. j) destruir claves. k) hacer seguimiento y auditorias de las actividades relacionadas con la gestión de las claves.
	P2	**Autenticidad de claves públicas** Comprobar la autenticidad de la claves públicas mediante una autoridad certificadora
Documentos por revisar	D1	Documentos de acuerdos de nivel de servicio.
	D2	Contratos con proveedores de servicios criptográficos

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.4.**	**Seguridad de los archivos del sistema**
Control	**12.4.1.**	**Control del software en producción.**
Objetivo	Existencia de procedimientos para controlar la instalación del software en sistemas operacionales.	
Procedimientos Específicos	P1	**Actualización de librerías** Verificar que sólo el administrador capacitado, previa autorización de la gerencia, realiza la actualización de las librerías de programas operativos
	P2	**Sistemas operativos** Verificar que los sistemas operativos solo tengan código ejecutable y no desarrollo de código o compiladores.
	P3	**Implantación con pruebas** Verificar que no se implante código en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuentes.
	P4	**Sistemas operativos** Constatar la utilización de un sistema de control de configuración para mantener un control de todo el software implementado así como la documentación del sistema.
	P5	**Estrategia de restauración** Verificar existencia de una estrategia de restauración no actualizada antes de que se implementen los cambios.
	P6	**Registros de auditoría** Comprobar la retención de las versiones anteriores como medida de precaución.
	P7	**Retención de versiones anteriores.** Verificar que se archivan las versiones antiguas de software junto con toda la información requerida, los parámetros, procedimientos, detalles de configuración y software de soporte, durante el tiempo en que los datos.
	P8	**Archivar registros de auditorías.** Verificar que son archivadas las versiones antiguas del software junto con la información requerida, los parámetros, procedimientos, detalles de configuración y software de soporte, durante el tiempo en que los datos sean retenidos.
Documentos por revisar	D1	Informes de auditoria
	D2	Documento de estrategia de restauración.

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.4.**	**Seguridad de los archivos del sistema**
Control	**12.4.2.**	**Protección de los datos de prueba del sistema**
Objetivo	Los datos de prueba deben ser seleccionados cuidadosamente, así como protegidos y controlados.	
Procedimientos Específicos	P1	**Procedimientos de control de acceso** Comprobar que los procedimientos de control de acceso que se consideran para las aplicaciones del sistema operacional son utilizados también en los sistemas de aplicaciones en prueba.
	P2	**Copiado de información operativa** Verificar que se autoriza por separado cada vez que se copia información operativa a un sistema de aplicación o en prueba.
	P3	**Borrado de información operativa** Verificar que se borra la información operativa de la aplicación del sistema en prueba en cuanto ésta se complete
	P4	**Registro de copiado y uso de información operativa** Verificar que se registra la copia y uso de la información operativa a efectos de seguimiento para auditoria
Documentos por revisar	D1	Registros de copiado y uso de información operativa
	D2	Documentos de procedimientos de control de acceso a aplicaciones del sistema operacional

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.4.**	**Seguridad de los archivos del sistema**
Control	**12.4.3.**	**Control de acceso a los códigos de programas fuente**
Objetivo	El acceso a los códigos de programas fuente debe ser restringido.	
Procedimientos específicos	P1	Verificar que las librerías de programas fuentes no deberían residir en los sistemas operativos
	P2	Constatar que el código y librería de programas fuente es maniobrado de acuerdo a procedimientos establecidos
	P3	Comprobar que el personal de apoyo informático no tenga libre acceso, sin restricción, a las librería de programas fuentes.
	P4	Verificar que la actualización de librerías de programas y la entrega de programas a los programadores se realiza sólo por el responsable con autorización del gerente de soporte informático para la aplicación
	P5	Verificar que los listado de programas se mantiene en un entorno seguro (véase 10.7.4.)
	P6	Comprobar que se mantiene un registro de auditoria de todos los accesos a las librerías de programas fuentes.
	P7	Constatar que el mantenimiento y copia de librerías de programas fuente estén sujetos a procedimientos estrictos de control de cambios (véase 12.5.1.)
Documentos por revisar	D1	Registros de auditoria de accesos a librerías de programas fuentes
	D2	Documento de responsabilidades y roles de seguridad
	D3	Actas de uso de códigos y librerías de programas fuente.
	D4	Procedimientos de control de cambios

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.5.**	**Seguridad en los procesos de desarrollo y soporte**
Control	**12.5.1.**	**Procedimientos de control de cambios**
Objetivo	La implementación de cambios debe ser controlada usando procedimientos formales de cambio.	
Procedimientos Específicos	P1	**Proceso de control de cambios** Verificar que el proceso de control de cambios incluye una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios. Que no se comprometa la seguridad y los procedimientos de control existentes, que los programadores de soporte se les de acceso solo a las partes del sistema necesarias para su trabajo y que se tenga aprobación y acuerdo formal para cualquier cambio.
	P2	**Aplicación y procedimiento de control de cambios integrados** Verificar que la aplicación y sus procedimientos de control de cambios estén integrados siempre que sea posible (véase 10.1.2.). Esto incluye: a) el mantenimiento de un registro de los niveles de autorización acordados. b) la garantía de que los cambios se realizan por usuarios autorizados. c) la revisión de los controles y los procedimientos de integridad para asegurarse que los cambios no los debilitan. d) la identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora. e) la obtención de la aprobación formal para propuestas detalladas antes de empezar el trabajo. f) la garantía de la aceptación por el usuario autorizado de los cambios antes de cualquier implantación. g) la garantía de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua. h) el mantenimiento de un control de versiones de toda actualización del software. i) el mantenimiento de un seguimiento de auditoría de todas las peticiones de cambio. j) la garantía del cambio de la documentación operativa (véase el inciso 10.1.1) y de los procedimientos de usuario en función de la necesidad. k) la garantía de la adecuación del tiempo de implantación de los cambios para no dificultar los procesos de negocio implicados.
Documentos por revisar	D1	Documento de gestión de cambios.
	-	-

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.5.**	**Seguridad en los procesos de desarrollo y soporte**
Control	**12.5.2.**	**Revisión técnica de los cambios en el sistema operativo**
Objetivo	Revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad	
Procedimientos Específicos	P1	**Procedimientos de control de la aplicación y de la integridad** Verificar que se haya dado la revisión de los procedimientos de control de la aplicación y de la integridad para asegurar que los cambios en el sistema operativo no han sido comprometidos
	P2	**Revisiones y pruebas del sistema** Verificar cubre la garantía que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema que requieran los cambios del sistema operativo
	P3	**Modificación de los cambios del sistema operativo** Comprobar que cubre la garantía de que la modificación de los cambios del sistema operativos se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación
	P4	**Aplicación y procedimiento de control de cambios integrados** Revisar que cubre la garantía de que se realizan los cambios apropiados en los planes de continuidad del negocio (véase 14.)
Documentos por revisar	D1	Documento del proceso de cambios en el sistema operativo
	D2	Procedimientos de control de la aplicación y de la integridad

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.5.**	**Seguridad en los procesos de desarrollo y soporte**
Control	**12.5.3.**	**Restricciones en los cambios a los paquetes de software**
Objetivo	No se recomiendan modificaciones a los paquetes de software. Se debería limitar a cambios necesarios y todos estos deben ser estrictamente controlados.	
Procedimientos Específicos	P1	**Debilitamiento de medidas de control e integridad** Verificar que se tomó en cuenta el riesgo de debilitamiento de las medidas de control incorporadas y sus procesos de integridad
	P2	**Consentimiento del vendedor** Comprobar que se tomó en cuenta la obtención del consentimiento del vendedor
	P3	**Actualizaciones normales** Verificar que se tuvo en cuenta la posibilidad de obtener los cambios requeridos como actualizaciones normales del programa del vendedor
	P4	**Análisis de impacto** Verificar que se tomó en cuenta el impacto causado si la organización adquiere la responsabilidad del mantenimiento futuro del software como resultado de los cambios
Documentos por revisar	D1	Documento de análisis de impacto por el cambio del paquete del software
	D2	Procedimientos de control de la aplicación y de la integridad

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.5.**	**Seguridad en los procesos de desarrollo y soporte**
Control	**12.5.4.**	**Fuga de información**
Objetivo	Las oportunidades de fuga de información deben ser prevenidas	
Procedimientos Específicos	P1	**Riesgo de fuga de información** Verificar que se limita el riesgo de fuga de información
Documentos por revisar	D1	Documento de riesgos de fuga de información
	D2	Documento de controles para la fuga de información

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.5.**	**Seguridad en los procesos de desarrollo y soporte**
Control	**12.5.5.**	**Desarrollo externo del software**
Objetivo	El desarrollo externo del software debe ser supervisado y monitoreado por la organización.	
Procedimientos Específicos	P1	**Aspectos a considerar** Verificar que se consideró los siguientes aspecto cuando se externalice el desarrollo de software: a) acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual (véase el inciso 15.1.2). b) certificación de la calidad y exactitud del trabajo realizado. c) acuerdos para hacerse cargo en el caso de fallo de terceros. d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado. e) requisitos contractuales sobre la calidad y funcionalidad segura del código. f) pruebas antes de la implantación para detectar el código Troyano.
Documentos por revisar	D1	Documento de procedimientos para el desarrollo externo del software
	D2	Acuerdos bajo licencia
	D3	Contratos con entidad desarrolladora del software
	D4	Documento de pruebas del software

Dominio	**12**	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
Categoría	**12.6.**	**Gestión de la vulnerabilidad técnica**
Control	**12.6.1.**	**Control de las vulnerabilidades técnicas.**
Objetivo	Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar a los riegos asociados.	
Procedimientos Específicos	P1	Verificar que una acción apropiada y a tiempo sea tomada en cuenta en respuesta a la identificación de vulnerabilidades técnicas potenciales. Las siguientes pautas se siguen para establecer un proceso de gestión de vulnerabilidades técnicas efectivas: a) la organización debe definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquier otra responsabilidades coordinadas. b) los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre ellos se deben identificar para el software y otras tecnologías (basadas en el inventario de activos, véase 7.1.1); estos recursos de información deben ser actualizados basados en cambios de inventario o cuando un recurso nuevo o mas útil se encuentre. c) se debería definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes. d) una vez identificada las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Esta acción puede implicar el parchado de sistemas vulnerables y/o la aplicación de otros controles. e) dependiendo en que tan urgente sea necesario tratar una vulnerabilidad técnica,la acción a ser tomada en cuenta debe ser llevada a cabo de acuerdo a controles relacionados con la gestión de cambios (véase el inciso 12.5.1) o siguiendo los procedimientos de respuesta ante incidentes en la seguridad de información (véase el inciso 13.2). f) si un parche se encuentra disponible, se deben tratar los riesgos asociados con la instalación (los riesgos planteados por la vulnerabilidad deben ser comparados con los riesgos de instalación del parche). g) los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos y que no resulten en efectos secundarios que no puedan ser tolerados; si no existe ningún parche disponible, se deberían considerar otros controles como: 1) apagar los servicios y capacidades relacionadas con la vulnerabilidad. 2) adaptar o tratar los controles de acceso, por ejemplo los firewall en los bordes de red (véase el inciso 11.4.5). 3) monitoreo creciente para detectar o prevenir ataques actuales.

		4) aumento en la precaución de la vulnerabilidad. h) un registro de ingreso debe ser mantenido para todos los procedimientos emprendidos. i) se debería monitorear y evaluar la gestión de procesos en la vulnerabilidad técnica con el fin de asegurar su efectividad y eficiencia. j) los sistemas en alto riego deben ser tratados primero.
Documentos por revisar	-	-
	-	-

4.9. DOMINIO 13: Gestión de incidentes en la seguridad de información

Dominio	**13.**	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
Categoría	**13.1.**	**Reportando eventos y debilidades de la seguridad de información**
Control	**13.1.1.**	**Reportando los eventos en la seguridad de información**
Objetivo	Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de una gestión de canales apropiada	
Procedimientos Específicos	P1	**Retroalimentación** Verificar que existan procesos de retroalimentación adecuados para asegurar que dichos eventos reportados de la seguridad de información sean notificados de los resultados después de que el tema haya sido repartido y cerrado.
	P2	**Formularios de reporte** Comprobar que existan formularios de reporte de eventos en la seguridad de información, con el fin de apoyar la acción de reporte y para ayudar a la persona que reporta recordar todas las acciones necesarias en caso de un evento.
	P3	**Comportamiento** Constatar la existencia de un comportamiento correcto a ser emprendido en caso de un evento en la seguridad de información, por ejemplo: 1) notar todos los detalles importantes (tipos de no conformidad, mal funcionamiento, aberturas, mensajes en la pantalla, conducta extraña) inmediatamente. 2) no llevar a cabo ninguna acción por si mismo, pero reportar inmediatamente al punto de contacto.
	P4	**Proceso disciplinario** Verificar la existencia de referencias a un proceso formal disciplinario establecido para tratar con empelados, contratistas o terceros que cometan una abertura en la seguridad
Documentos por revisar	D1	Reportes de eventos
	D2	Documentos de gestión de incidentes
	D3	Documentos de canales comunicación.

Dominio	**13.**	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
Categoría	**13.1.**	**Reportando eventos y debilidades de la seguridad de información**
Control	**13.1.2.**	**Reportando debilidades en la seguridad de información**
Objetivo	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y reportar cualquier debilidad observada o sospechada en la seguridad de estos.	
Procedimientos Específicos	P1	**Política de conformidad de derechos de autor del software.** Constatar la publicación de una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.
	P2	**Asegurar Copyright en software adquirido** Adquisición de software mediante fuentes conocidas para asegurar que el copyright no sea violado.
Documentos por revisar	D1	Reportes de eventos
	D2	Documentos de gestión de incidentes
	D3	Documentos de canales comunicación.

Dominio	**13.**	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
Categoría	**13.2.**	**Gestión de las mejoras e incidentes en la seguridad de información**
Control	**13.2.1.**	**Responsabilidades y procedimientos**
Objetivo	Las responsabilidades y procedimientos de la gerencia deben ser establecidas para asegurar una rápida, efectiva y ordenada respuesta a los incidentes en la seguridad de información	
Procedimientos Específicos	P1	Verificar que los procedimientos son establecidos para diferentes tipos de incidentes en la seguridad de información como por ejemplo: 1) fallas y pérdidas de servicio en los sistemas de información. 2) código malicioso (véase el inciso 10.4.1). 3) negación de servicio. 4) errores resultantes de datos incompletos o no actualizados. 5) aperturas en la confidencialidad e integridad. 6) mal uso de los sistemas de información.
	P2	Verificar que en adición a los planes de contingencias normales, los procedimientos también cubran: 1) análisis e identificación de la causa del incidente. 2) contención. 3) si es necesario, planeamiento e implementación de acciones correctivas para prevenir la re ocurrencia. 4) comunicaciones con lo afectados o implicados en recuperarse del incidente. 5) reportar acciones a la autoridad apropiada.
	P3	Verificar que exista un registro de auditorías, recolección de evidencia similar y reguardada para: 1) análisis de problemas internos. 2) el uso de evidencia forense en relación con una apertura potencial del contrato, requisitos regulados o en el caso de procedimientos civiles o criminales, como por ejemplo el mal uso del computador o la legislación de protección de datos. 3) negociaciones para compensaciones por parte de los proveedores de software o del servicio.
	P4	Constatar que existan acciones para recuperarse de aperturas de seguridad y controlar, formal y cuidadosamente, las fallas del sistema que han sido corregidas. Los procedimientos aseguran que:

		1) solo el personal claramente identificado y autorizado están permitidos de acceder a los sistemas y datos vivos (véase también 6.2 para acceso externo). 2) todas las acciones de emergencia que se realizaron sean documentadas a detalle. 3) las acciones de emergencia sean reportadas a la gerencia y revisados de una manera ordenada. 4) la integridad de los sistemas y controles de negocio son confirmados con un mínimo de retraso.
Documentos por revisar	D1	Documento de Responsabilidades y procedimientos
	D2	Documento de gestión de incidentes

Dominio	**13.**	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
Categoría	**13.2.**	**Gestión de las mejoras e incidentes en la seguridad de información**
Control	**13.2.2.**	**Aprendiendo de los incidentes en la seguridad de información**
Objetivo	Debe existir un mecanismo que permita que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.	
Procedimientos Específicos	P1	**Identificación de incidentes frecuentes o de gran impacto** Verificar que la información ganada de la evaluación de los incidentes en la seguridad de información es utilizada para identificar incidentes que se repiten o de gran impacto.
Documentos por revisar	D1	Documento de gestión de incidentes
	D2	Registro de incidentes de la organización

Dominio	**13.**	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**
Categoría	**13.2.**	**Gestión de las mejoras e incidentes en la seguridad de información**
Control	**13.2.3.**	**Recolección de evidencia**
Objetivo	Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante.	
Procedimientos Específicos	P1	**Admisibilidad de evidencia: si es que la evidencia puede ser utilizada en corte** Verificar que se asegura que sus sistemas de información cumplen con cualquier estándar o código publicado de práctica para la producción de evidencia admisible.
	P2	**Corte en la evidencia: Calidad y lo completo de la evidencia** Comprobar que la calidad y lo completo de los controles usados para corregir y proteger consistentemente la evidencia (como por ejemplo el proceso de control de evidencia) durante el periodo en que la evidencia que se recupera se almacena y se procesa, está demostrado por un fuerte seguimiento de dicha evidencia. En general, dicho seguimiento puede ser establecido bajo las siguientes condiciones: a) para documentos en papel: el original es guardado con seguridad con un registro del individuo que encontró el documento, donde se encontró, cuando fue encontrado y quien presenció dicho descubrimiento. Cualquier investigación debe asegurar que los originales no hayan sido forzados. b) para información en medios informáticos: se deben de tomar en cuenta imágenes espejo o copias (dependiendo de los requerimientos aplicables) de cualquier medio removible, información en discos duros o en memoria con el fin de asegurar la disponibilidad. El registro de todas las acciones durante el proceso de copiado debe ser mantenido y el proceso debe ser presenciado; el medio original y el registro (si este no es posible, al menos con imágenes espejo o copias) debe ser mantenido de una forma segura e intocable.
	P3	**Integridad de material en evidencia** Verificar que la integridad de todo el material en evidencia es protegida. Las copias son supervisadas por personal confiable y se registra la información de cuando y donde fue ejecutado el proceso de copia, quien realizó dichas actividades y que herramientas y programas se utilizaron.
Documentos por revisar	D1	Documento de evidencias
	D2	Procedimientos para la protección de la integridad de la evidencia
	D3	Documento legislativos, regulatorios y contractuales.

4.10. DOMINIO 14: Gestión de continuidad de negocio

Dominio	**14.**	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
Categoría	**14.1.**	**Aspectos de la gestión de continuidad del negocio.**
Control	**14.1.1.**	**Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio**
Objetivo	Instalar en toda la organización un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del negocio a través de la organización que trate los requerimientos en la seguridad de la información necesarios para la continuidad del negocio.	
Procedimientos Específicos	P1	**Comprender los riesgos** Constatar que se identificó todos los activos implicados en los procesos críticos de negocio.
	P2	**Impacto** Constatar que se comprende el impacto que tendrían las interrupciones en el negocio y se establecen los objetivos del negocio en lo referente a los medios informáticos.
	P3	**Adquisición de seguros** Verificar la consideración de la adquisición de los seguros adecuados que formarán parte del proceso general de continuidad del negocio y parte de la gestión operacional de riesgo.
	P4	**Implementación de controles adicionales** Comprobar la identificación y consideración de implementar controles adicionales de prevención.
	P5	**Recursos financieros, organizacionales, técnicos y ambientales.** Comprobar la identificación de los recursos financieros, organizacionales, técnicos y ambientales necesarios para realizar los requisitos identificados de seguridad de información.
	P6	**Seguridad del personal y de la organización** Verificar el aseguramiento de la seguridad del personal y la protección de las instalaciones de procesamiento y de la propiedad de la organización.
	P7	**Planes de continuidad de Negocio (BCP)** Confirmar la existencia de planes de continuidad de negocio en línea con la estrategia acordada en el control 14.1.3.
	P8	**Prueba y actualización de los BCPs** Verificar que los planes y procesos de continuidad del negocio instalados sean probados y actualizados regularmente.

	P9	**Gestión de continuidad de negocio** Constatar que la gestión de la continuidad del negocio se incorpora en los procesos y estructura de la organización.
Documentos por revisar	D1	Planes de continuidad del negocio de la organización
	D2	Documentos de responsabilidades en la gestión de BCPs
	D3	Documento de activos implicados en procesos críticos del negocio
	D4	Documento de riesgos
	D5	Adquisiciones de seguros
	D6	Documento de implementación de controles adicionales de prevención

Dominio	**14.**	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
Categoría	**14.1.**	**Aspectos de la gestión de continuidad del negocio.**
Control	**14.1.2.**	**Continuidad del negocio y evaluación de riesgos**
Objetivo	Identificar los eventos que pueden causar interrupciones a los procesos de negocio, junto con la probabilidad de impacto de dichas interrupciones y sus consecuencias para la seguridad de información	
Procedimientos Específicos	P1	**Identificar eventos** Constatar que se identificó los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de negocio, por ejemplo, una falla del equipo, una inundación o un incendio.
	P2	**Evaluación del riesgo** Constatar que se evaluó el riesgo para determinar la probabilidad e impacto de los eventos llevada a cabo con una total implicancia por parte de los propietarios de los recursos y procesos de negocio.
	P3	**Plan estratégico de la continuidad del negocio** Constatar que se desarrolló un plan estratégico para determinar un enfoque global de la continuidad del negocio a partir de los resultados de la evaluación del riesgo. Además del respaldo de la gerencia.
Documentos por revisar	D1	Documento de riesgos
	D2	Plan estratégico de la continuidad del negocio

Dominio	**14.**	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
Categoría	**14.1.**	**Aspectos de la gestión de continuidad del negocio.**
Control	**14.1.3.**	**Redacción e implantación de planes de continuidad que incluyen la seguridad de información**
Objetivo	Desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos.	
Procedimientos Específicos	P1	**Procedimientos de emergencia y responsabilidades** Verificar la identificación de los procedimientos de emergencia y los acuerdos de todas las responsabilidades para la continuidad del negocio.
	P2	**Pérdidas aceptables** Verificar la identificación de las pérdidas aceptables de información y servicios.
	P3	**Procedimientos de recuperación y restauración.** Constatar la implementación de procedimientos que permitan la recuperación y restauración de las operaciones de negocio y la disponibilidad de información en escalas de tiempo requerido.
	P4	**Procedimientos para complementar la recuperación y restauración** Constatar la implementación de procedimientos operacionales de seguimiento para complementar la restauración y recuperación.
	P5	**Procedimientos y procesos acordados.** Verificar que exista la documentación de los procedimientos y procesos acordados.
	P6	**Formación del personal en los procedimientos y procesos acordados.** Comprobar la formación apropiada del personal en los procedimientos y procesos de emergencia acordados, incluyendo la gestión de crisis.
	P7	**Prueba y actualización de los BCPs** Constatar la prueba y actualización de los planes de continuidad de negocio.
Documentos por revisar	D1	Planes de continuidad del negocio de la organización
	D2	Documento de pérdidas aceptables de información y servicios.
	D3	Documento de procedimientos de recuperación y restauración.
	D4	Documento de gestión de crisis

Dominio	**14.**	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
Categoría	**14.1.**	**Aspectos de la gestión de continuidad del negocio.**
Control	**14.1.4.**	**Marco de planificación para la continuidad del negocio**
Objetivo	Mantener un esquema único de planes de continuidad del negocio para asegurar que los planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.	
Procedimientos Específicos	P1	**Condiciones para activar los planes** Verificar que se detallen las condiciones para activar los planes que describen el proceso a seguir antes de dicha activación (cómo evaluar la situación ,quiénes tiene que estar implicados, etc.)
	P2	**Procedimientos de emergencia** Verificar que se describan las acciones a realizar tras una contingencia que amenace las operaciones del negocio (procedimientos de emergencia).
	P3	**Procedimientos de respaldo.** Comprobar que se especifique las acciones a realizar para desplazar de forma temporal a lugares alternativos las actividades esenciales del negocio o soportar servicios y para devolver la operatividad a los procesos del negocio.
	P4	**Procedimientos temporales de operación.** Comprobar que se definan los procedimientos temporales de operación para seguir con las terminaciones pendientes de reanudación y restauración
	P5	**Procedimientos de reanudación.** Constatar que se describan las acciones a realizar para que las operaciones del negocio vuelvan a su normalidad.
	P6	**Calendario de mantenimiento** Verificar que se especifique cómo y cuándo se harán pruebas del plan, así como el proceso de su mantenimiento.
	P7	**Concientización y formación** Corroborar que se detallen las actividades de concientización y formación diseñadas para comprender los procesos de continuidad del negocio y asegurar que los procesos prosigan con eficacia.
	P8	**Responsabilidades** Constatar que se describa a cada responsable de la ejecución de cada etapa del plan.
	P9	**Activos y recursos críticos para realizar los procedimientos.**

		Comprobar si se cuenta con los activos y recursos críticos necesarios para poder realizar los procedimientos de emergencia, respaldo y reactivación
Documentos por revisar	D1	Planes de continuidad del negocio de la organización
	D2	Documentos de responsabilidades en la gestión de BCPs
	D3	Documento de activos implicados en realizar los procedimientos.
	D4	Documento de riesgos

Dominio	**14.**	**GESTIÓN DE CONTINUIDAD DEL NEGOCIO**
Categoría	**14.1.**	**Aspectos de la gestión de continuidad del negocio.**
Control	**14.1.5.**	**Prueba, mantenimiento y revaluación de los planes de continuidad**
Objetivo	Probar regularmente los planes de continuidad del negocio para asegurarse de su actualización y eficacia.	
Procedimientos Específicos	P1	**Prueba sobre el papel de varios escenarios** Verificar el análisis de las disposiciones de recuperación del negocio con ayuda de ejemplos de interrupciones.
	P2	**Simulaciones** Comprobar que el personal gestiona la crisis tras la contingencia
	P3	**Recuperación técnica** Verificar que los sistemas de información pueden restaurarse con efectividad.
	P4	**Recuperación en un lugar alternativo** Comprobar el funcionamiento de los procesos del negocio en paralelo con las operaciones de recuperación fuera del lugar principal
	P5	**Prueba de los recursos y servicios del proveedor** Constatar que los servicios externos proporcionados cumplen el compromiso contraído.
	P6	**Ensayos completos** Comprobar que se hace frente a las interrupciones de la organización, el personal, los recursos y los procesos.
Documentos por revisar	D1	Contrato con proveedores relacionados a los BCPs
	D2	Planes de continuidad del negocio.
	D3	Documento de anteriores pruebas y evaluaciones de los BCPs

4.11. DOMINIO 15: Cumplimiento

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.1.**	**Identificación de la legislación aplicable**
Objetivo	Definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información.	
Procedimientos Específicos	P1	**Revisión de parámetros generales de la seguridad de la información.** Verificar que los controles, medidas y responsabilidades estén definidos y documentados para cumplir los requisitos legales en el Perú
Documentos por Revisar	D1	Documento de requisitos legales, regulatorios y contractuales para cada sistema de información.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.2.**	**Derechos de propiedad intelectual**
Objetivo	Implementar procedimientos para asegurar el cumplimiento de las restricciones legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual y software propietario.	
Procedimientos Específicos	P1	**Política de conformidad de derechos de autor del software.** Constatar la publicación de una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.
	P2	**Asegurar Copyright en software adquirido** Adquisición de software mediante fuentes conocidas para asegurar que el copyright no sea violado.
	P3	**Concientizar sobre derechos de autor del software y políticas de adquisiciones.** Comprobar la difusión en la cultura organizacional sobre los derechos de autor del software y la política de adquisiciones
	P4	**Registrar apropiadamente los activos.** Verificar la protección los derechos de propiedad intelectual mediante la identificación de todos los activos con requerimientos y mantener los registros apropiados de activos.
	P5	**Documentación de propiedad de licencias, originales, manuales.** Verificar la existencia de documentos que acrediten la propiedad de licencias, material original, manuales, etc.
	P6	**Asegurar número máximo de usuarios permitidos.** Constatar la publicación de una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.
	P7	**Instalación solamente de software autorizado y productos bajo licencia** Comprobar que sólo haya instalado software autorizado y productos bajo licencia.
	P8	**Mantenimiento de las condiciones de la licencia.** Verificar que se tenga establecido una política de mantenimiento de las condiciones adecuadas de la licencia.
	P9	**Eliminación de software o de su transferencia a terceros.** Comprobar que se tenga establecida una política de eliminación de software o de su transferencia a terceros.
	P10	**Auditoría** Comprobar el uso de herramientas adecuadas de auditoría
	P11	**Términos y condiciones de uso del software e información de redes públicas** Constatar el cumplimiento de los términos y condiciones de uso del software y de la información obtenida de redes

		públicas.
	P12	**Prohibiciones por la ley de copyright (analógica o digital)** Verificar que no se hayan duplicado, convertido en otro formato o extraído de grabados comerciales (audio, filmaciones) lo que no sea permitido por la ley de copyright.
	P13	**Prohibiciones por la ley de copyright (físico, papel)** Verificar que no se hayan copiado parcial o totalmente libros, artículos, reportes u otros documentos que no sean permitidos por la ley de copyright.
Documentos por revisar	D1	Términos y condiciones del software (Licencia)
	D2	Documento de requisitos legislativos, regulatorios y contractuales.
	D3	Documentación de propiedad intelectual (que incluyen al software o copyright del documento, derechos de diseño, marca registrada, patente y fuentes de licencia de código)

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.3.**	**Salvaguarda de los registros de la organización**
Objetivo	Proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.	
Procedimientos Específicos	P1	**Guías de retención, almacenamiento, tratamiento y eliminación de los registros y la información.** Comprobar que se hayan publicado guías sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información.
	P2	**Calendario de retenciones** Verificar que se hayan establecido un calendario de retenciones que identifique los períodos para cada tipo esencial de registros.
	P3	**Inventario de las fuentes clave.** Verificar que se haya mantenido un inventario de las fuentes de información clave.
	P4	**Controles y medidas** Constatar que se hayan implementado controles y medidas apropiadas para la protección de los registros y la información esencial contra su pérdida, destrucción o falsificación.
Documentos por revisar	D1	Registros contables, de base de datos, de transacciones, de auditoria.
	D2	Documento de requisitos legislativos, regulatorios y contractuales.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.4.**	**Protección de los datos y de la privacidad de la información personal**
Objetivo	Asegurar la protección de datos y privacidad como se requiere en la legislación, reguladores y, si es aplicable, en las cláusulas contractuales.	
Procedimientos Específicos	P1	**Política Organizacional de privacidad y protección de datos** Constatar la implementación y desarrollo de una política organizacional y de protección de datos, que haya sido comunicada a todo el personal implicado.
	P2	**Ley de protección de datos personales** Verificar que se haya implementado medidas técnicas y organizacionales apropiadas para proteger la información personal
Documentos por revisar	D1	Documento de Política Organizacional
	D2	Documento de requisitos legislativos (ley de protección de datos personales), regulatorios y contractuales.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.5.**	**Prevención en el mal uso de los recursos de tratamiento de la información**
Objetivo	Disuadir al personal de utilizar los recursos informáticos de la información para propósitos no autorizados.	
Procedimientos Específicos	P1	**Considerar impropio uso de recursos para fines no autorizados.** Constatar que se haya adoptado la acción disciplinaria y/o legal apropiada cuando se identificó el uso de recursos para fines no autorizados o ajenos al negocio.
	P2	**Usuarios conscientes del alcance preciso del acceso que se les permite** Verificar si todos los usuarios son conscientes del alcance preciso del acceso que se les permite y del monitoreo que se lleva a cabo para detectar un uso no autorizado.
	P3	**Mensajes de advertencia del sistema** Corroborar si al registrarse un usuario, un mensaje de advertencia indica en la pantalla que el sistema al que se entra es privado y que no se permite el acceso no autorizado.
Documentos por revisar	D1	Documentos de uso de recursos de tratamiento de la información
	D2	Políticas de detección de intrusos
	D3	Documento de requisitos legislativos, regulatorios y contractuales.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.1.**	**Cumplimiento con los requisitos legales**
Control	**15.1.6.**	**Regulación de los controles criptográficos**
Objetivo	Utilizar en conformidad con todos los acuerdos, leyes y regulaciones los controles criptográficos	
Procedimientos Específicos	P1	**Importación y/o exportación para realizar funciones criptográficas** Corroborar la conformidad de las restricciones en la importación y/o explotación de hardware y software para realizar funciones criptográficas con todos los acuerdos, leyes y regulaciones
	P2	**Importación y/o exportación que incluya funciones criptográficas** Corroborar la conformidad de las restricciones en la importación y/o explotación de hardware y software para realizar funciones criptográficas con todos los acuerdos, leyes y regulaciones.
	P3	**Uso del encriptado** Verificar que las restricciones en el uso del encriptado esté en conformidad con todos los acuerdos, leyes y regulaciones
	P4	**Métodos para acceder a información cifrada** Verificar existan métodos obligatorios o discrecionales para acceder a la información que esté cifrada por hardware o software para proteger la confidencialidad de su contenido
Documentos por revisar	D1	Documentos de los métodos para acceder a información cifrada
	D2	Documento de requisitos legislativos, regulatorios y contractuales.
	D3	Documentos de las restricciones sobre el encriptado.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.2.**	**Revisiones de la política de seguridad y de la conformidad técnica**
Control	**15.2.1.**	**Conformidad con la política de seguridad y los estándares.**
Objetivo	Asegurar que se cumplan correctamente todos los procedimientos de seguridad.	
Procedimientos Específicos	P1	**Revisiones regulares de las políticas y normas de seguridad** Verificar que la gerencia haya realizado revisiones regulares que aseguren el cumplimiento de las políticas de seguridad
	P2	**Tratamiento de no conformidad** Verificar que la gerencia determinó las causas de la no conformidad, evaluó las acciones para asegurar que no vuelva a ocurrir, determinó e implementó una acción correctiva apropiada y revisó la acción correctiva que realizó.
	P3	**Grabado y mantenimiento de revisiones** Constatar que los resultados de las revisiones y de las acciones correctivas llevadas a cabo por los gerentes debes ser grabados y mantenidos.
	P4	**Reporte de resultados de revisiones independientes** Constatar que los gerentes reporten los resultados de las revisiones a las personas que llevan a cabo las revisiones independientes, cuando dicha revisión es llevada a cabo en el área de su responsabilidad.
Documentos por revisar	D1	Documentos de las revisiones de las políticas y normas de seguridad realizadas.
	D2	Reportes de resultados de revisiones.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.2.**	**Revisiones de la política de seguridad y de la conformidad técnica**
Control	**15.2.2.**	**Comprobación de la conformidad técnica**
Objetivo	Comprobar regularmente la conformidad con las normas de implantación de la seguridad en los sistemas de información	
Procedimientos Específicos	P1	**Conformidad técnica** Verificar que la comprobación de la conformidad técnica haya sido realizada manualmente por un ingeniero de sistemas experimentado (con apoyo de herramientas lógicas apropiadas si es necesario), o bien automáticamente por un paquete que genere un informe técnico, a interpretar posteriormente por el especialista técnico.
	P2	**Evaluaciones de vulnerabilidad** Comprobar que las pruebas de intrusión o evaluaciones de vulnerabilidad hayan sido planeadas, documentadas y repetibles.
	P3	**Competencias de supervisores** Comprobar que las personas que realicen o supervisen la comprobación de la conformidad técnica sean competentes y autorizadas.
Documentos por revisar	D1	Documentación de las comprobaciones de conformidad técnica.
	D2	Documentos que sustenten las competencias y autorizaciones de los supervisores.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.3.**	**Consideraciones sobre la auditoria de sistemas**
Control	**15.3.1.**	**Controles de auditoria de sistemas**
Objetivo	Planificar cuidadosamente y acordarse los requisitos y actividades de auditoria que impliquen comprobaciones en los sistemas operativos, para minimizar el riesgo de interrupción de los procesos de negocio.	
Procedimientos Específicos	P1	**Requisitos de auditoria** Constatar que se haya acordado los requisitos de auditoría con la gerencia apropiada
	P2	**Alcance de auditoria** Verificar que se acordó y controló el alcance de las verificaciones
	P3	**Acceso de las verificaciones** Constatar que las verificaciones se limitaron a accesos solo de lectura al software y a los datos.
	P4	**Acceso distintos a solo lectura** Verificar que los accesos distintos a solo lectura, únicamente se permitió para copias aisladas de archivos del sistema y que se borró cuando se terminó la auditoria.
	P5	**Recursos de TI para las verificaciones** Constatar que los recursos de Tecnología de la Información para realizar verificaciones son explícitamente identificados y puestos a disposición.
	P6	**Requisitos para procesos especiales** Verificar que los requisitos para procesos especiales o adicionales son identificados y acordados.
	P7	**Registro de accesos** Comprobar que todos los accesos estén registrados y supervisados para producir un seguimiento de referencia. El uso de seguimiento de referencia de tiempo es considerado para sistemas o datos críticos.
	P8	**Procedimientos, requisitos y responsabilidades** Comprobar que todos los procedimientos, requisitos y responsabilidades estén documentados.
	P9	**Independencia de los auditores** Verificar que las personas que llevan a cabo la auditoria deban ser independientes de las actividades auditadas.
Documentos por revisar	D1	Documento de procedimientos, requisitos y responsabilidades
	D2	Documento de registro de accesos.
	D3	Informes de auditoria.

Dominio	**15.**	**CUMPLIMIENTO**
Categoría	**15.3.**	**Consideraciones sobre la auditoria de sistemas**
Control	**15.3.2.**	**Protección de las herramientas de auditoria de sistemas**
Objetivo	Proteger los accesos a las herramientas de auditoria de sistemas con el fin de prever cualquier posible mal uso o daño.	
Procedimientos Específicos	P1	**Herramientas de auditoria de sistemas separadas o con protección adicional** Verificar que las herramientas de auditoria de sistemas, por ejemplo, software o archivos de datos, estén separadas de los sistemas de desarrollos y de producción y no en librerías de cintas o en áreas de los usuarios, salvo con un nivel apropiado de protección adicional.
Documentos por revisar	D1	-
	D2	-