TECNOLOGÍA DE LOS PODERES JUDICIALES

CONTENIDO

1. Seguridad de la Información

La información es un activo que tiene un alto valor y requiere, en consecuencia, una protección adecuada. Ésta se puede presentar de las siguientes formas:

- impresa o escrita en papel,
- almacenada electrónicamente,
- trasmitida por correo o medios electrónicos,
- hablada en conversación.

La seguridad de la información consiste en procesos y controles diseñados para protegerla de su divulgación no autorizada, transferencia, modificación o destrucción, a efecto de:

- asegurar la continuidad del negocio,
- minimizar posibles daños, y
- maximizar oportunidades.

La seguridad informática debe entenderse en el contexto de la seguridad física y lógica de la información, y por eso intenta proteger cuatro elementos:

- Hardware
- Software
- Datos
- Elementos Consumibles

2. Seguridad de Información Familia ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), estas normas incluyen:

1. **ISO/IEC 27000**- es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.
2. **ISO/IEC 27001** - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
3. **ISO/IEC 27002** - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. **Es un código de buenas prácticas para la gestión de seguridad de la información**. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
4. **ISO/IEC 27003** - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
5. **ISO/IEC 27004** - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
6. **ISO/IEC 27005** - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.
7. **ISO/IEC 27006:2007** - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
8. **ISO/IEC 27007** - Es una guía para auditar al SGSI. Se encuentra en preparación.
9. **ISO/IEC 27799:2008** - Es una guía para implementar ISO/IEC 27002 en la industria de la salud.
10. **ISO/IEC 27035:2011 -** Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este estándar hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

3. Seguridad de Información (ISO/IEC 27001)

Estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques – Information security management systems - Requirements)

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

PILARES DE SEGURIDAD DE INFORMACIÓN (ISO/IEC 27001)

4. Seguridad de Información (ISO/IEC 27002)

Es un conjunto de recomendaciones sobre qué medidas tomar en la institución para asegurar los Sistemas de Información.

Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009. Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita.

- Los **objetivos de seguridad** recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa.
  Para conseguir cada uno de estos objetivos, la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva se aplican para la gestión del riesgo analizado.

Los **objetivos de control** son los aspectos a asegurar dentro de cada área/sección; y los **controles** son los mecanismos para asegurar los objetivos de control (guía de buenas prácticas). Para cada control establecido, se debe elaborar una guía para su implantación)

Para la elaboración del documento que se presentará como guía de seguridad informática es conveniente utilizar la ISO/IEC 27002, en virtud que incluye controles específicos relacionados con aspectos informáticos.

4.1 Contenido de la norma

- ✓ 11 dominios
- ✓ 39 objetivos de control
- ✓ 133 controles

Los 133 controles y 39 objetivos están agrupados dentro de los 11 dominios descritos abajo:

DOMINIO		DESCRIPCIÓN
5.	Política De Seguridad	El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.
6.	Aspectos Organizativos de La Seguridad de la Información	La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.
7.	Gestión de Activos.	Inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial.
8.	Seguridad Ligada a los Recursos Humanos.	Los roles y responsabilidades de la seguridad debieran ser definidos y claramente comunicados a los candidatos para el puesto durante el proceso de pre-empleo.

DOMINIO		DESCRIPCIÓN
9.	Seguridad Física y del Entorno	Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.
10.	Gestión de Comunicaciones y Operaciones.	Procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.
11.	Control de Acceso.	Establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.
12.	Adquisición, Desarrollo y Mantenimiento De Sistemas de Información.	Identificary acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.
13.	Gestión de Incidentes en la Seguridad de la Información.	Procedimientos formales de reporte y de la intensificación de un evento, ejemplo: cambios del sistema no controlados, mal funcionamiento del software o hardware, violaciones de acceso.
14.	Gestión de la Continuidad del Negocio.	Desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
15.	Cumplimiento.	Definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

4.2 Guía de Seguridad Informática

Para el desarrollo de la guía en cuestión, se tomarán de referencia 5 dominios, los cuales se relacionan directamente con el área informática:

No.	DOMINIO
7.	Gestión de Activos.
10.	Gestión de Comunicaciones y Operaciones.
11.	Control de Acceso.
12.	Adquisición, Desarrollo y Mantenimiento De Sistemas de Información.
13.	Gestión de Incidentes en la Seguridad de la Información.

Guía de Seguridad Informática
ISO/IEC 27002

DOMINIO 7: GESTIÓN DE ACTIVOS

Activos.-

- **Información:** Bases de datos, la data (sorteo, providencias o actos procesales, sentencias, jurisprudencia; información administrativa, información financiera), contratos y acuerdos, resoluciones, planes de continuidad del negocio, registros de auditorías
- **Archivos de Software:** sistemas de gestión de trámite jurisdiccional, sistemas de gestión documentas, erp, sistemas operativos, entre otros.
- **Activos de Hardware:** Servidores, equipos de comunicación, equipamiento de TIC´s
- **Personal:** roles y responsabilidades acorde a la capacidad y experiencia del personal de las diferentes unidades de TIC´s
- **Intangibles:** Imagen de transparencia, celeridad, seguridad y justicia.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
7.1	Inventario de activos	Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.	La organización identificará todos los activos y documentará de acuerdo a su importancia. El inventario incluirá toda la información necesaria para recuperarse de los desastres.	El no contar con un conjunto de políticas específicas así como responsables para el uso de los activos podría verse afectada la integridad y disponibilidad de la información.
	Responsable de los activos	Toda la información y los activos asociados con los servicios de procesamiento de información deben ser asignada a una parte de la organización que actúa como responsable.	Una vez que se ha definido, identificado, elaborado el inventario de todos los activos de Tics de la organización se identificará al responsable o los responsables de controlar el uso y seguridad de estos. Además se realizará una revisión periódica a la clasificación y definición de responsables de los activos y servicios que se ofrecen.	
	Uso aceptable de los activos	Se debe identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.	Las organizaciones establecerán un conjunto de políticas, normas específicas, reglas, manuales de uso y demás directrices, con el fin de garantizar la seguridad y disponibilidad respecto al acceso y uso que se dé a los activos, asociados a los sistemas de información de cada una de las organizaciones.	
7.2	Directrices de clasificación	Se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.	Las organizaciones clasificarán la información en términos de valor, confidencialidad y criticidad para la organización, y será revisada periódicamente manteniéndose actualizada. La clasificación debe ser lo más sencilla y práctica en lo posible.	Al no existir una clasificación acorde a la importancia de la información así como el etiquetado según estándares internos adoptados para la organización podría verse afectada seriamente la integridad, disponibilidad y confidencialidad de la información.
	Etiquetado y manejo de la información	Se debe desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	Se debe definir un estándar de etiquetado adecuado de la información aprobado por la organización, que comprenda los formatos físicos y electrónicos. De acuerdo al nivel de importancia de la información se debe definir procedimientos de manejo seguro, así como el registro de incidentes de seguridad referido a la cadena de custodia.	

DOMINIO 10: GESTIÓN DE COMUNICACIONES Y OPERACIONES

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
10.1	Procedimientos y responsabilidades operacionales	Procedimientos de operación documentados	Preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación;	Falta de segregación de funciones.
		Gestión del cambio	Sistemas operacionales y el software de aplicación sujetos a un estricto control de autoridades del cambio.	
		Segregación de los deberes	Tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección.	
		Separación de los medios de desarrollo, prueba y operación	Identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales e implementar los controles apropiados.	
10.2	Gestión de la entrega del servicio de terceros	Entrega del servicio	Incluir acuerdos de seguridad pactados en la entrega del servicio por un tercero e incluir definiciones del servicio y aspectos de la gestión del servicio.	Falta de calidad en el servicio adquirido.
		Monitoreo y revisión de los servicios de terceros	El monitoreo y revisión de los servicios de terceros debiera asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información.	
		Manejo de cambios en los servicios de terceros	El proceso de manejar los cambios en el servicio de terceros necesita tomarlos cambios realizados por la organización	
10.3	Planeación y aceptación del sistema	Gestión de la capacidad	Identificar los requerimientos de capacidad de cada actividad nueva y en proceso.	Fallas de Operación en los sistemas
		Aceptación del sistema	Asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados.	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
10.4	Protección contra el código malicioso y móvil	Controles contra códigos maliciosos	Basarse en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio.	Posible pérdida de información y atraso en las operaciones.
		Controles contra códigos móviles	Considerar acciones para evitar que el código móvil realice acciones no-autorizadas	
10.5	Respaldo o Back-Up	Respaldo o Back-Up	Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios.	Posible pérdida de información crítica y suspensión de actividades
10.6	Gestión de seguridad de la red	Controles de redes	Implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.	Posible intrusión de terceros no autorizados e interrupción del servicio.
		Seguridad de los servicios de la red	Determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura	
10.7	Gestión de medios	Gestión de medios removibles	Considerar lineamientos para la gestión de medios removibles	Posible fuga de información.
		Retirada de soportes	Definición de procedimientos formales para la eliminación de medios confidenciales que ya no serán requeridos.	
		Procedimientos para el manejo de información	Establecer procedimientos para el manipuleo, procesamiento, almacenaje y comunicación de la información consistente con su clasificación.	
		Seguridad de la documentación del sistema	asegurar la documentación del sistema de manera segura	
10.8	Intercambio de información	Políticas y procedimientos de intercambio de información	Definir procedimientos y controles a seguirse cuando se utilizan medios de comunicación electrónicos para el intercambio de información	Posible fuga de información y suplantación de identidades.
		Acuerdos de intercambio	Establecer y mantener las políticas, procedimientos y estándares para proteger la información y medios físicos en tránsito	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
		Medios físicos en tránsito	Considerar lineamientos para proteger los medios de información transportados entre diferentes ubicaciones	
		Mensajes electrónicos	Definir consideraciones de seguridad para los mensajes electrónicos	
		Sistemas de información	Definir consideraciones a las implicancias de seguridad en la interconexión de los sistemas de información	
10.9	Comercio electrónico	Comercio electrónico	Definir consideraciones de seguridad para el comercio electrónico	Posibles transacciones fraudulentas
		Transacciones en-línea	Definir consideraciones de seguridad para Transacciones en-línea	
		Información públicamente disponible	Proteger mediante mecanismos apropiados el software, data y otra información que requiere un alto nivel de integridad, puesta a disposición en un sistema públicamente disponible,	
10.10	Monitoreo	Registro de auditoría	Considerar registros de auditoría cuando sea relevante.	Posible incapacidad de prevenir fallos de sistemas
		Uso del sistema de monitoreo	Determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo.	
		Protección del registro de información	Establecer controles para protegerse contra cambios no autorizados y problemas operacionales,	
		Registros del administrador y operador	Revisados de manera regular los registros de administrador y operador del sistema.	
		Registro de fallas	Registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación	
		Sincronización de relojes	Colocar la hora del reloj de acuerdo a un estándar acordado	

DOMINIO 11: CONTROL DE ACCESO

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
11.1	Requerimiento para el control del acceso	Política de control del acceso	Establecer claramente en la política de control de acceso las reglas de control del acceso y los derechos para cada usuario o grupos de usuarios.	Posibles accesos no autorizados.
11.2	Gestión de acceso del usuario	Registro del usuario	Definir el procedimiento de control del acceso para el registro y des-registro del usuario.	Posible otorgamiento inadecuado de permisos
		Gestión de privilegios	Controlar la asignación de privilegios a través de un proceso de autorización formal para los sistemas multi-usuario que requieren protección contra el acceso no autorizado.	
		Gestión de las claves secretas de los usuarios	Definir políticas sobre la gestión de las claves secretas, medio común para verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de información en concordancia con la autorización del usuario	
		Revisión de los derechos de acceso del usuario	Definir lineamientos para la revisión de los derechos de acceso	
11.3	Responsabilidades del usuario	Uso de claves secretas	Formular política para la el uso de claves secretas de los usuarios	Posible perdida y fuga de información
		Equipo del usuario desatendido	Estar al tanto de los requerimientos de seguridad y los procedimientos para proteger el equipo desatendido por parte de los usuarios.	
		Política de escritorio y pantalla limpios	Tomar en cuenta las clasificaciones de información para políticas de escritorio limpio y pantalla limpia.	
11.4	Control de acceso a la red	Política sobre el uso de los servicios de la red	Formular una política relacionada con el uso de las redes y los servicios de la red.	Posible pérdida y fuga de información e interrupción de actividades.
		Autenticación del usuario para las conexiones externas	Utilizar técnicas basadas en criptografía, dispositivos de hardware o un protocolo de desafío/respuesta para la autenticación de los usuarios remotos.	
		Identificación del equipo en las redes	Utilizar la identificación del equipo si es importante que la comunicación sólo sea iniciada desde una ubicación o equipo específico.	
		Protección del puerto de diagnóstico y configuración remoto	Uso de un seguro y procedimientos de soporte para controlar el acceso físico al puerto que incluya controles potenciales para el acceso a los puertos de diagnostico y configuración.	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
		Segregación en redes	Un método para controlar la seguridad de grandes redes es dividirlas en dominios de red lógicos separados	
		Control de conexión a la red	Los derechos de acceso a la red de los usuarios se debieran mantener y actualizar conforme lo requiera la política de control de acceso	
		Control de routing de la red	Implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones	
11.5	Control del acceso al sistema operativo	Procedimientos para un registro seguro	Diseño del procedimiento para registrarse en un sistema de operación de manera que minimice la oportunidad de un acceso no autorizado.	Posible suspensión de actividades y del servicio.
		Identificación y autenticación del usuario	Aplicar este control a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos).	
		Sistema de gestión de claves secretas	Los sistemas para el manejo de claves secretas debieran ser interactivos y debieran asegurar claves secretas adecuadas.	
		Uso de las utilidades del sistema	Se debieran considerar lineamientos para el uso de las utilidades del sistema:	
		Cierre de una sesión por inactividad	Un dispositivo de cierre debiera borrar la pantalla de la sesión y también, posiblemente más adelante, cerrar la aplicación y las sesiones en red después de un período de inactividad definido.	
		Limitación del tiempo de conexión	considerar controles sobre el tiempo de conexión para las aplicaciones de cómputo sensibles,	
11.6	Control de acceso a la aplicación y la información	Restricción del acceso a la información	Las restricciones para el acceso se debieran basar en los requerimientos de las aplicaciones.	Posible fuga y pérdida de información
		Aislar el sistema confidencial	considerar los siguientes lineamientos para aislar el sistema sensible o confidencial	
11.7	Computación y tele-trabajo móvil	Computación y comunicaciones móviles	Establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.	Posible suplantación de identidad y accesos no autorizados.

DOMINIO 12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
12.1	Requisitos de seguridad de los sistemas de información	Análisis y especificación de los requisitos de seguridad	Definir de líneas base de seguridad en aplicaciones e infraestructura de TI, de acuerdo a la necesidad de cada aplicación.	Posible adquisición e implementación de sistemas que no cumplen con medidas de seguridad reconocidas o aprobadas por la Institución.
12.2	Tratamiento correcto de las aplicaciones	Validación de los datos de entrada.	Validar los datos de entrada para evitar errores por captura de datos incorrectos.	Posible liberación en ambiente productivo de aplicaciones con vulnerabilidades de seguridad y procesamiento de datos incorrecto.
		Control de procesamiento interno	Revisar la seguridad de las aplicaciones a nivel código para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.	
		Integridad de los mensajes	Evaluar los riesgos de seguridad para determinar si se requiere la integridad del mensaje e identificar el método de implementación más apropiado.	
		Validación de los datos de salida	Validar los datos en el procesamiento, para asegurar que la información almacenada sea la correcta y la apropiada para las circunstancias. Ya que aún en los sistemas que han sido probados se puede producir output incorrecto.	
12.3	Controles Criptográficos	Política de uso de controles criptográficos	Desarrollar e implementar una Política para el uso de controles criptográficos, para proteger la información.	Posible afectación a la confidencialidad de la información mantenida en los sistemas y aplicaciones de la Institución. Posible falsificación de la firma digital, reemplazándola con la clave pública de un usuario.
		Gestión de claves	Proteger las claves criptográficas contra una modificación, pérdida y destrucción. Proteger contra la divulgación no-autorizada, las claves secretas y privadas. Brindar seguridad física al equipo utilizado para generar, almacenar y archivar las claves. A manera de ejemplo, los dos tipos de técnicas criptográficas son:	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			técnicas de claves secretas y técnicas de claves públicas.	
12.4	Seguridad de los archivos de sistema	Control del Software en explotación	Minimizar el riesgo de corrupción de los sistemas operacionales, considerando lineamientos para controlar los cambios como son: actualización del software operacional, los sistemas operacionales sólo deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores. Establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios.	Posibles fugas y pérdidas de información confidencial en posesión de la Institución, que pueden ser utilizadas para fines ajenos a la misma.
		Protección de los datos de prueba del sistema	Para los propósitos de pruebas, evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial. Autorizar por separado cada vez que se copia información operacional en un sistema de aplicación de prueba.	
		Control de acceso al código fuente de los programas	El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se deben controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados. Implementar procedimientos estrictos de control de cambios para el mantenimiento y copiado de las bibliotecas fuentes del programa.	
12.5	Seguridad en los procesos de desarrollo y soporte	Procedimientos de control de cambios	Documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas existentes deben realizarse después de un proceso formal de documentación, especificación, prueba,	Posible introducción de cambios no probados y no autorizados en los sistemas y aplicaciones de la Institución. Posibles problemas de segregación de funciones en desarrollo y operación. Posible fuga de Información.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			control de calidad e implementación manejada. La buena práctica incluye la prueba del software nuevo en un ambiente segregado de los ambientes de producción y desarrollo.	
		Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Revisar y probar las aplicaciones comerciales críticas, cuando se cambian los sistemas de operación, para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad. Asignar a un grupo o persona específica la responsabilidad de monitorear las vulnerabilidades, así como los parches y arreglos que lancen los vendedores.	
		Restricciones a los cambios en los paquetes de software	Limitar los cambios necesarios y controlarlos estrictamente. Utilizar los paquetes de software suministrados por vendedores sin modificaciones.	
		Fugas de Información	Considerar puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos (covertchannels). Tomar medidas para protegerse contra códigos Troyanos reduce el riesgo de la explotación de los canales encubiertos.	
		Externalización del desarrollo de software	Supervisar y monitorear, el desarrollo del software abastecido externamente. Considerar puntos como contratos de licencias, propiedad de códigos, derechos de propiedad intelectual.	
12.6	Gestión de la vulnerabilidad técnica	Control de las vulnerabilidades técnicas	Obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados. Un inventario actual y completo de los activos (ver 7.1) es un	Posible incapacidad para detectar problemas de seguridad en los sistemas y aplicaciones de la Institución. Posible incapacidad para tomar las medidas necesarias de contención, y responder oportunamente.

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			prerrequisito para la gestión efectiva de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, números de la versión, estado actual del empleo (por ejemplo, cuál software está instalado en cuál sistema), y la(s) persona(s) dentro de la organización responsable(s) del software.	

DOMINIO 13.GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
13.1	Notificación de eventos y puntos débiles de seguridad de la información	Notificación de los eventos de seguridad de la información	Reportar a través de los canales gerenciales apropiados lo más rápidamente posible los eventos de seguridad de la información. Tomar la conducta correcta en el caso de un evento en la seguridad de la información; por ejemplo: No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto.	Posible incapacidad para detectar problemas de seguridad en los sistemas y aplicaciones de la Institución. Incapacidad para tomar las medidas necesarias de contención, y responder oportunamente.
		Notificación de puntos débiles de seguridad	Requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios. El mecanismo de reporte debe ser fácil y estar disponible.	
13.2	Gestión de incidentes y mejoras de seguridad de la información	Responsabilidades y procedimientos	Establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.	
		Aprendizaje de los incidentes de seguridad de la información	Establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información. Analizar la información obtenida para identificar los incidentes recurrentes o de alto impacto.	
		Recopilación de evidencias	Recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s). Desarrollar y seguir los procedimientos	

No.	OBJETIVO DE CONTROL	CONTROL	ACCIÓN	RIESGO
			internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización. Realizar en las copias del material de evidencia cualquier trabajo forense. Lo anterior aplica por ejemplo, para una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal);	

4.3 Fases de desarrollo

La implementación de dicha guía debe incluir el desarrollo de objetivos, políticas, procesos y procedimientos, considerando las siguientes definiciones para su elaboración:

5. Tecnología, dimensionamiento y sus costos

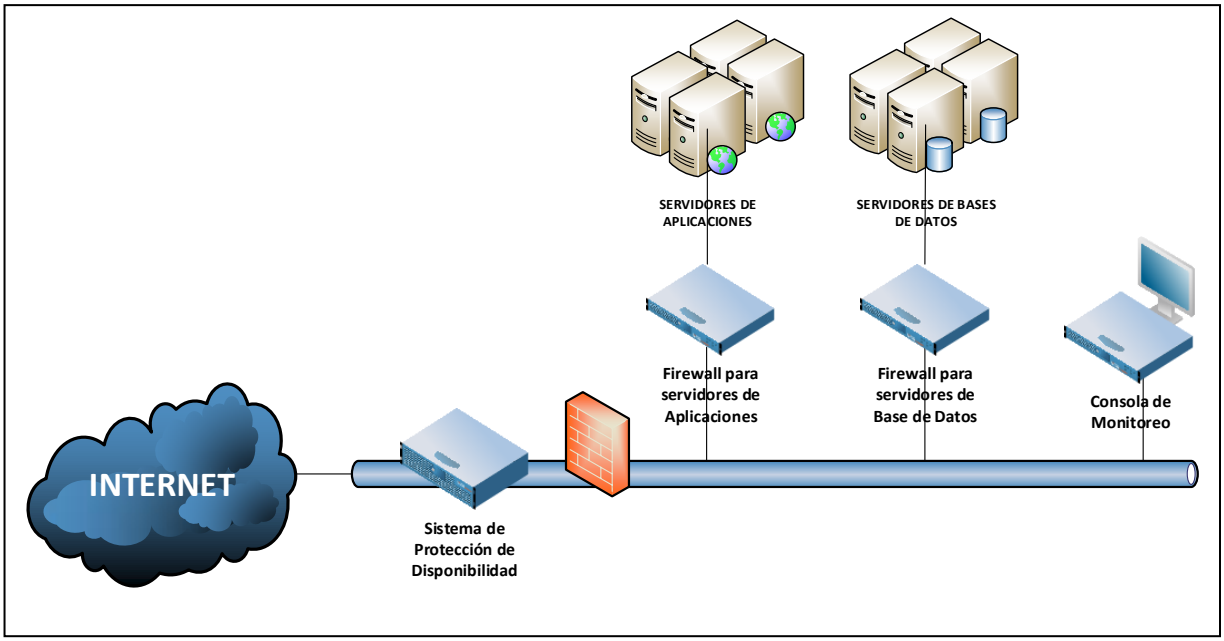
En general se recomienda que se adopten tecnologías para brindar seguridad en las siguientes áreas:

Esquemas de Seguridad	
Área	**Aplicativo / Software**
Escritorio	Antivirus, Antispyware, FireWall Personal IPS local, Filtro Web, Control de Acceso a Red, Dispositivos Móviles Control de Aplicaciones / Listas Blancas/Negras
Datos	Encripción de disco, Encripción de archivos, Control de Dispositivos Prevención de fuga de información local, Prevención de fuga de información en la red, Administración de permisos, Respaldo y Restauración, Almacenamiento Empresarial (SAN)
Servidor	Antivirus, Antispyware, FireWall local IPS local, Filtro Web, Control de Acceso a Red, Control de Aplicaciones / Listas Blancas/Negras, Virtualización
Red	Firewall perimetrales, Prevención de Intrusos, Firewall de Aplicaciones, Control de Acceso a Red, Análisis de Comportamiento, Análisis Forense, Control de Infraestructura.
Correo	Antispam, Antivirus, Prevención de Fuga de Información
Internet	Filtro de Contenidos, Proxy, Antivirus, Antimalware.
Riesgo y Cumplimiento	Manejador de Vulnerabilidades, Remediador de Vulnerabilidades, Auditoria de Políticas, Análisis y reporte de Riesgo, Control de Cambios, Monitor de Integridad de Archivos, SIEM, Manejador de Logs

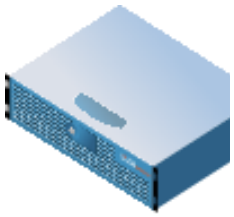
5.1 Casos prácticos

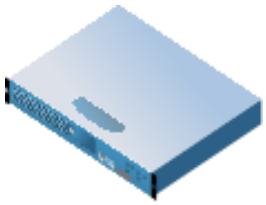
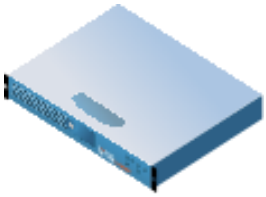
CASO 1

Esquema de seguridad:



ALTA SEGURIDAD - BENEFICIOS POR COMPONENTE:

 **Sistema de Protección de Disponibilidad**	• Protege, desde Internet, las aplicaciones de amenazas de seguridad, combinando en una defensa cohesiva diversos mecanismos de seguridad. • Con esta herramienta se evita que ataques maliciosos vulneren los sistemas y saturen los servidores con la finalidad de bloquear el servicio. • Ofrece actualizaciones para garantizar protección ante patrones de ataque y garantiza la disponibilidad de los servicios que se ofrecen en la organización.

 **Firewall para servidores de Aplicaciones**	• Ofrece el servicio de seguridad autoadaptable, sin saturar los servidores de aplicaciones, entregando una solución de alta seguridad que garantiza la integridad de la información y las aplicaciones web. • Con este componente es posible monitorear en tiempo real, la información que se transmite a través de las aplicaciones web. • Automáticamente aprende el comportamiento de las aplicaciones y de sus usuarios, detectando comportamientos anormales y alertando de ellos en tiempo real. • Identifica el tráfico que es originado por robots y Fuentes maliciosas conocidas, para detener ataques automatizados. • Previene fraudes vía web con su funcionalidad “ThreatRadarFraudPrevention”.
 **Firewall para servidores de Base de Datos**	• Protege a las Bases de Datos de ataques, pérdida y robo de información a través de un monitoreo en tiempo real con el cual, se emiten alertas y bloqueos de acceso basados en políticas de seguridad preestablecidas y que pueden ser configurables según nuestras necesidades. • Es posible controlar y monitorear quién tiene el acceso a las bases de datos y a la información que se accedió, teniendo pleno control de la consulta de la información. • Con este componente de infraestructura se protegerá uno de los recursos más valiosos de la Institución que es la información.
 **Consola de Monitoreo**	• La consola de monitoreo alerta de posibles ataques en cualquiera de los componentes de seguridad instalados y ofrece información detallada de las acciones realizadas en la detención de ataques. • Así mismo, recaba información forense de los intentos de ataque a la infraestructura resguardada.

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
12.1	Requisitos de seguridad de los sistemas de información	Número de servidores Número de usuarios Número de direcciones IP	Herramientas de blindaje para sistema operativo Herramienta de Seguridad en Control de Cambios Herramientas de Pruebas de Penetración automatizada Herramienta Análisis de vulnerabilidades	(~520K USD)
12.2	Tratamiento correcto de las aplicaciones	Número de desarrolladores de aplicaciones Número de aplicaciones y tamaño de estas Número de direcciones IP	Servidores de aplicaciones Servidores de bases de datos Firewall para servidores de aplicaciones Firewall para servidores de bases de datos Consola de monitoreo Sistema de protección de disponibilidad	(~19,743,750USD)
12.3	Controles Criptográficos	Número de aplicaciones a integrar en el bus criptográfico ya sean legacy o de terceros. Número de sistemas que manejan certificados digitales SSL o llaves de SSH (F5, firewalls, BlueCoat, web, servidores, etc.)		

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
12.4	Seguridad de los archivos de sistema	Número de aplicaciones, servidor(es) donde se encuentra instalada la base de datos, tamaño de la base de datos Número de base de datos, segmentos de red, número de sites Número de sistemas a integrar (Switches, Sistemas operativos, bases de datos, etc.) Número de servidores Unix o Windows Número de endpoints, Número de usuarios		
12.5	Seguridad en los procesos de desarrollo y soporte	Número de servidores virtuales y número de hypervisors Número de sistemas a integrar (Switches, Sistemas operativos, bases de datos, etc.) Número de endpoints, Número de salidas a Internet		
12.6	Gestión de la vulnerabilidad técnica	Número de direcciones IP		
13.1	Notificación de eventos y puntos débiles de seguridad de la información	Número de Segmentos de red Numero de bases de datos y transacciones por base de datos, Throughput Número de aplicaciones web Número de correo saliente en hora pico / Número y tamaño de los enlaces a Internet Período de retención, Número de enlaces de red, Número de dispositivos de red con sus eventos por		

No.	OBJETIVO DE CONTROL	PUNTOS CLAVE PARA DIMENSIONAMIENTO	TECNOLOGÍAS HW/SW	PRECIO
		segundo		
13.2	Gestión de incidentes y mejoras de seguridad de la información	Organigrama de la institución Período de retención, Número de enlaces de red, Número de dispositivos de red con sus eventos por segundo Número de administradores de servicios		

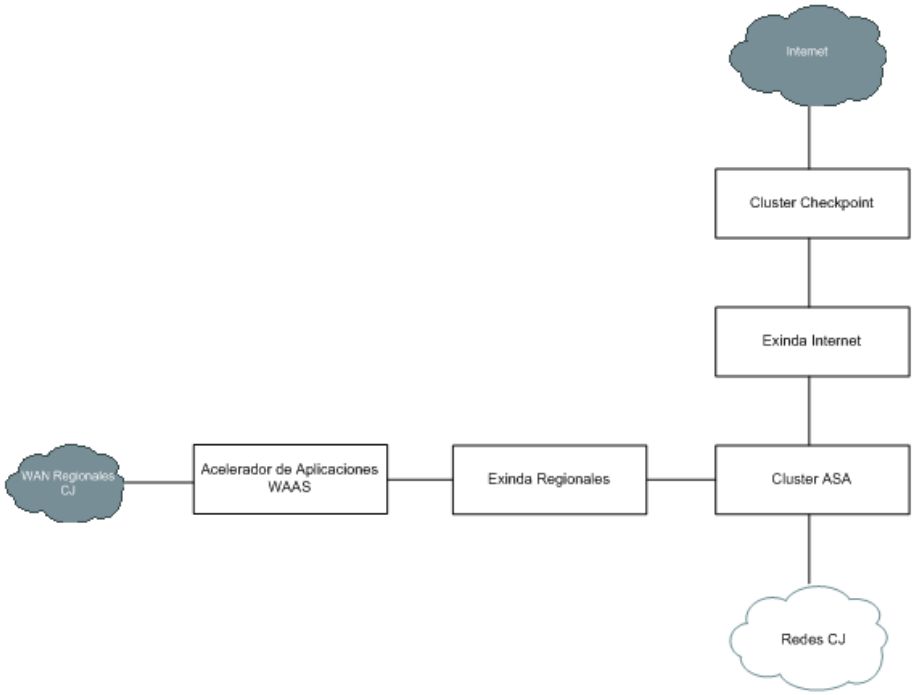
CASO 2

El caso de éxito más importante ha sido la implementación de un Data Center, en donde se centraliza todo el equipamiento y la aplicación de políticas de seguridad, de acuerdo a la recomendación de buenas prácticas, modelos y metodologías adoptadas en consultorías efectuadas para la implementación de la ISO 27000.
Se recomienda adoptar la estandarización de equipos en cada una de las regionales, lo que permite que las políticas sean de fácil aplicación, pues el manejo de protocolos comunes representa una gran ventaja.
Adicionalmente se debe implementar un Data Center Alterno de iguales características en otra regional, lo que permite la replicación de toda la información y garantiza la alta disponibilidad de todas las aplicaciones.
La inversión aproximada en equipamiento y Data Center ha sido de: USD 25'000.000

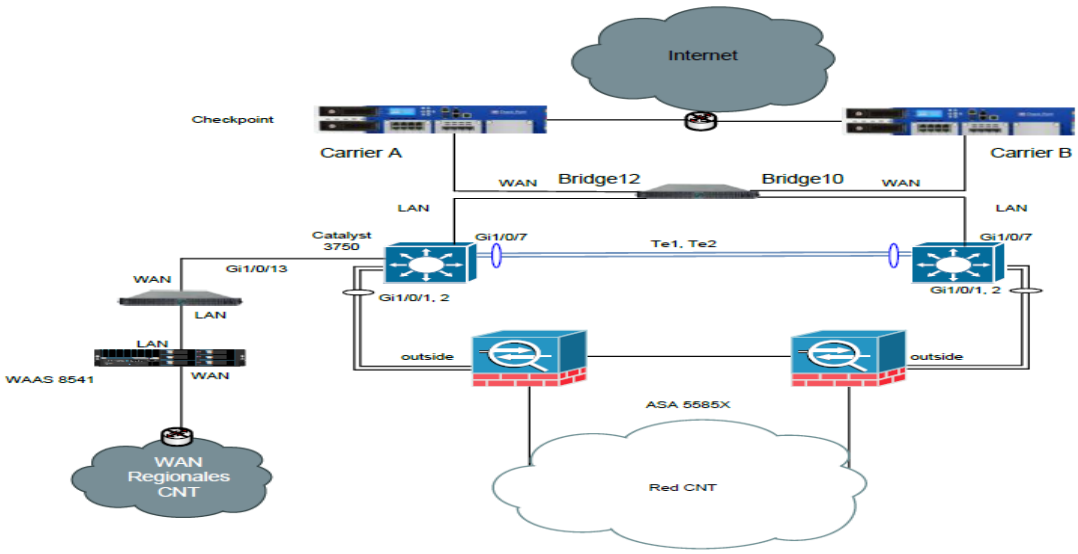
SISTEMA DE SEGURIDAD INFORMATICA

SEGURIDAD PERIMETRAL		
Seguridad de acceso web	Exinda	Administrador de ancho de banda
Seguridad de acceso web	Checkpoint	Filtrado Web
Seguridad de correo electrónico	IronPortmail - Cisco	Antispam
Seguridad de autenticación	ASA - Cisco	Firewall, IPS
Optimización de tráfico	Cisco- Wave	WASS - Acelerador de tráfico
Autenticación	Cisco - ACS	Autenticación activos equipos de red
Gestión de aplicaciones	Cisco- ACE	Balanceador de carga
SEGURIDAD INTERNA		
Acceso a servidores de aplicación	Cisco - VCG	Seguridad de acceso a aplicaciones en ambiente virtual
Antivirus	MacAfee	Protección antivirus
Protección de equipos	Microsoft - WSUS	Distribución de parches y actualizaciones
Protección de equipos	Red Hat-Satellite	Distribución de parches y actualizaciones
Protección de equipos de activos	Cisco - ACL	Configuración de funcionalidades de seguridad en equipos activos
Autenticación de usuarios	Microsoft- GPO Active Directory	Configuración de políticas de Grupo para la autenticación de usuarios en el directorio activo
Protección de red inalámbrica	Cisco - WirelessLanController	Configuración de grupos y niveles de seguridad para la autenticación de usuarios a la red inalámbrica, configurando las funcionalidades de la controladora a la que se anexan los accesspoint

TOPOLOGI SEGURIDAD DEL DATACENTER



ESQUEMA DE EQUIPAMIENTO SEGURIDAD DATACENTER



COSTOS APROXIMADOS

Los valores descritos a continuación son referenciales y están ligados a otras soluciones de tecnología informática, por ejemplo en los equipos activos adicionalmente a su funcionalidad de brindar los elementos de conectividad, permiten la configuración de políticas de seguridad como listas de acceso y calidad de servicio para el tráfico que pasa por la red como la telefonía IP.

SEGURIDAD	INVERSIÓN APROXIMADA
Equipamiento de seguridad perimetral	5'000.000,00
Licenciamiento antivirus	1´000.000,00
Consultorías de seguridad	500.000,00
Equipamiento activo y comunicaciones	18'000.000,00
Equipamiento para servidores para autenticación y políticas de seguridad	1'000.000,00