SGSI

E.S.E HOSPITAL REGIONAL CENTRO

INTRODUCCION

La norma internacional ISO/IEC 27000 es un conjunto de estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información de las personas o empresas interesadas y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La información es un activo valioso que puede impulsar o destruir una empresa. Si se gestiona de forma adecuada, permite trabajar con confianza. La gestión de la Seguridad de la Información ofrece la libertad para crecer, innovar y ampliar la base de clientes sabiendo que toda la información siempre será de carácter confidencial.

Esta guía no pretende ser de cumplimiento obligatorio, sino informativa, proporcionando algunos requisitos de la norma y orientando respecto a la manera en que se pueden cumplir esos requerimientos.

Generalmente, una primera aproximación a la norma puede infundir desconfianza en cuanto a la capacidad de la empresa para poder llevar a cabo todos los requerimientos que expresa, debido a que la norma específica una amplia gama de controles de seguridad a implementaren numerosos casos con una gran carga de contenido técnico.

Esta guía pretende suplir algunas carencias en materia de seguridad de la información, proporcionando información detallada sobre las posibles actividades a desarrollar para cumplir y alcanzar dicho control.

Objetivo: Promover un sistema de gestión de la seguridad de la información (SGSI) en la E.S.E HOSPITAL REGIONAL CENTRO, Sede principal, que contemple las recomendaciones generales y actividades para la implantación dela seguridad de la información, aplicando la norma internacional ISO 27002.

ALCANCE: Este trabajo se presenta como una guía de buenas prácticas y recomendaciones para la gestión de la seguridad de la información, basada en la normativa ISO 27002, promoviendo un sistema de gestión de la Seguridad de la información (SGSI) dentro de la E.S.E Hospital Regional Centro.

DESCRIPCIÓN DEL ESQUEMA O FORMATO DE LA GUÍA: el desarrollo de las medidas de seguridad se realizara mediante el esquema en fichas, las cuales disponen los siguientes campos:

Dominio: Comprende las áreas de control o actuación según el estándar ISO 27002.

Objetivo: Conjunto de controles son una serie de consideraciones (controles) y un conjunto de sugerencias para cada uno de los controles.

Control: medios para manejar el riesgo, incluyen políticas, procedimiento, lineamientos, práctica; las cuales pueden ser administrativas, técnicas, de gestión o naturaleza legal.

DESARROLLO

Propósito: Hace referencia al control de la ISO 27002, el cual describe lo que se ha de proteger con su implementación.

Recomendación: Es un conjunto de sugerencias que permite llevar a cabo de una forma adecuada las acciones que orienten la implementación de los controles.

Actividades: son las acciones necesarias que se recomiendan para lograr la materialización del control, no todas son de cumplimiento obligatorio debido a que no lo requieren, para ello se formula una serie de estrategias como son:

- ✓ Políticas
- ✓ Procedimientos
- ✓ Formatos o formularios
- ✓ Uso de tecnologías (Hardware y Software)

GUÍA DE BUENAS PRÁCTICAS Y RECOMENDACIONES EN LA GESTIÓN DE LA SGURIDAD DE LA INFORMACIÓN

DOMINIO	Política de Seguridad	**OBJETIVO**	Directrices de la Dirección en seguridad de la información.
CONTROL	5.1.1 Conjunto de políticas para la seguridad de la información.		

DESARROLLO

Propósito: Establecer una política de seguridad con el fin de informar y concientizar a todos los empleados de la empresa sobre la estrategia de seguridad y definir las directrices generales de actuación para evitar amenazas ante incidentes que pongan en riesgo la seguridad de la información de la empresa.

Recomendación: La política de seguridad requiere un alto compromiso de la Gerencia, para que las medidas adoptadas sean efectivas, entre las principales medidas que han de tener respaldo directo están:

- ✓ Establecer una política de seguridad de la información
- ✓ Asegurar que se establezcan controles para el cumplimiento de la política.
- ✓ Establecer roles y responsabilidades para la seguridad de la información
- ✓ Comunicar a todos los empleados de la empresa la importancia de lograr los controles de seguridad de la información y cumplir la política de seguridad de la información, del cumplimiento de la ley y la necesidad de un mejoramiento continuo.
- ✓ Decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptable
- ✓ Realizar revisiones periódicas en el cumplimento de la política

Actividades:

- ✓ Difusión de la política a empleados de las diferentes IPS relevantes y una socialización con el resto de empleados de la empresa.
- ✓ Mantener una comunicación interna entre las diversas dependencias de la empresa acerca de la seguridad de la información, para mantener adecuadamente su funcionamiento y por ende asegurar el cumplimiento de la política y sus objetivos.
- ✓ La política debiera darse a conocer a través de los siguientes medios:
  - Publicación en sitios de acceso al personal empleado
  - Inducción a nuevos funcionarios contratados
  - Comunicaciones a través de charlas y reuniones de socialización
  - Publicación en el portal web oficial de la empresa.
  - Correo electrónico

- Oficios y circulares

DOMINIO	Política de Seguridad	**OBJETIVO**	Directrices de la Dirección en seguridad de la información.
CONTROL	5.1.2 Revisión política de seguridad de la información		

DESARROLLO

Propósito: La política de seguridad de la información puede ser revisada a intervalos de tiempos planeados, con la finalidad de asegurar su continua idoneidad, conveniencia y efectividad; esta revisión puede incluir una evaluación para el mejoramiento así como la necesidad de cambios en el sistema, incluyendo la política de seguridad y los objetivos de seguridad de la información.

Recomendación: La revisión de la política de seguridad de la información, pudiera ser reflejada en un informe de revisión el cual contenga los siguientes aspectos:

a) Mejoramiento de la efectividad en su aplicación.
b) Debería existir o estar conformado un comité de Seguridad de la información.
c) Actualización de la evaluación del riesgo y el plan de tratamiento de riesgo.
d) Modificaciones en los procedimientos y controles que afecten la seguridad de la información.
e) Detectar las necesidades de recursos para que en la medida de lo posible se puedan administrar de acuerdo a las prioridades y presupuesto disponible por la empresa.

Actividades: El Comité de Seguridad de la Información debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.
Efectuar toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

DOMINIO	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Organización interna.
CONTROL	6.1.1 Asignación de responsabilidades para la seguridad de la información.		

DESARROLLO

Propósito: Definir y asignar claramente todas las responsabilidades para la seguridad de la información. Establecer un marco de referencia gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la empresa.

Recomendación: Las personas con responsabilidades de seguridad asignadas pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo responsables y debieran determinar si cualquier tarea delegada ha sido realizada correctamente.
Debe estar aprobada la política de seguridad de la información por parte de la gerencia o a quien corresponda, para asignar los roles de seguridad, coordinar y revisar la implementación de la seguridad en toda la empresa.

Actividades:

- ✓ Documentar las actividades que sean ejecutadas en conformidad con la política de seguridad de la información.
- ✓ Identificar los procesos y activos de información relevantes y los distintos niveles de autorización para los activos de información identificados.
- ✓ Formalizar a los responsables por cada proceso/activo de información identificado.
- ✓ Creación, aprobación y aplicación de planes de capacitación y sensibilización para los empleados y funcionarios de la empresa.
- ✓ Monitorear y vigilar la implementación de los controles de seguridad en toda la empresa.

DOMINIO	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Organización interna.
CONTROL	6.1.2 Segregación de tareas		

DESARROLLO

Propósito: Reducir las oportunidades de una modificación no autorizada o intencionada o mal uso de los activos de la empresa.

Recomendación:
a) Cuidar de que nadie pueda tener acceso, modificar o utilizar los activos sin autorización previa.
b) Que existan procedimientos seguros para la iniciación de un evento en el sistema.
c) Definir en el diseño de los controles en el desarrollo de las tareas ejecutadas.
d) Realizar una auditoría de seguridad independiente a los demás dominios y objetivos.

Actividades:

- ✓ Crear perfiles de usuario que sean consecuentes con las descripciones del cargo que desempeñe cada empleado y que contengan únicamente el acceso a los sistemas de la información que requiere para llevar a cabo sus funciones.
- ✓ El encargado de seguridad debe validar estos perfiles y auditarlos al menos cada 6 meses.
- ✓ Separar la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas, mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
- ✓ Implementar controles y procedimientos que incluya:
  - Monitoreo de las actividades que realiza cada empleado.
  - Registros de auditoría y control periódico de los mismos.
  - Registro de amenazas por el acceso no autorizados desde los perfiles de usuarios asignados.

DOMINIO	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Organización interna.

CONTROL	6.1.3 Contacto con las autoridades

DESARROLLO

Propósito: mantener los contactos apropiados con las autoridades pertinentes.

Recomendación:
Mantener los contactos pertinentes se convierte en un requerimiento que apoya el manejo de un incidente de seguridad o la continuidad del negocio y el proceso de planeación de contingencia. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad; por ejemplo, departamento de bomberos, proveedores de telecomunicaciones y los proveedores de energía eléctrica.

Actividades:

- Mantener un registro de las empresas prestadoras de servicio tales como bomberos, defensa civil, proveedores de servicio, entre otros; donde se identifique claramente la persona de contacto, dirección y número telefónico.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Antes de la contratación.
CONTROL	7.1.1 Investigación de antecedentes		

DESARROLLO

Propósito: realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos de la empresa, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Recomendación:
Los chequeos de verificación de antecedentes de todos los candidatos para empleo, contratistas y terceros debieran llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes; y debieran ser proporcionales a los requerimientos productivos, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
Cuando un puesto de trabajo, sea un nombramiento inicial o un ascenso, involucra que la persona tenga acceso a los medios de procesamiento de información, y en particular si las personas manejan información confidencial; por ejemplo, información financiera o información altamente confidencial; la empresa también debe considerar chequeos más detallados.

Actividades: Realizar chequeos de verificación que incluyan:

- ✓ Disponibilidad de referencias de carácter satisfactorias tanto trabajadora como personal.
- ✓ Chequeo completo de la hoja de vida del postulante en cuanto a integridad y exactitud en la información suministrada.
- ✓ Confirmación de títulos académicos y profesionales mencionados por el postulante.
- ✓ Comprobación de la identidad del postulante.
- ✓ Solicitar certificados de antecedentes personales, disciplinarios y judiciales.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Antes de la contratación.
CONTROL	7.1.2 Términos y condiciones de contratación		

DESARROLLO

Propósito: Definir las funciones y responsabilidades de seguridad para cada uno de los usuarios de los sistemas de información; para ello es necesario establecer solo los privilegios necesarios para el desarrollo de dichas labores.

Recomendación: Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento.

El personal que dispone de acceso al sistema de información para el desarrollo de sus funciones, deben recibir información acerca de la obligación de mantener secreto profesional sobre los datos que conozca en el desarrollo de sus labores, aún después de finalizar la relación laboral que le une con la empresa, para ello es necesario establecer dentro de la contratación, acuerdos de confidencialidad en el que se informe de sus funciones y obligaciones respecto a la información de la empresa.

Actividades:

- ✓ Establecer acuerdos de confidencialidad para empleados y contratistas, antes de otorgarles acceso a los medios de procesamiento de la información.
- ✓ Documentar los acuerdos de confidencialidad para empleados y contratistas.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Durante la contratación
CONTROL	7.2.1 Responsabilidades de gestión		

DESARROLLO

Propósito: requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos por la empresa.

Recomendación: Se debe asegurar que todos los empleados, contratistas y terceras personas sean conscientes y estén apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información, para ello es necesario promover la divulgación y el conocimiento de la medidas de seguridad y de poner los medios formativos necesarios.

Dicha formación debiera abarcar los requisitos de seguridad, responsabilidades legales, objetivos de control, así como el uso adecuado de los recursos de tecnologías de la información con el objetivo de cumplir con las normas, estándares y otras directrices definidas en la política de seguridad.

Actividades:

- ✓ Educar al personal en materia de seguridad de la información, antes de otorgarles accesos a los activos de información.
- ✓ Realizar campañas de motivación y concientización para el cumplimiento de la política de seguridad, con el propósito de lograr un nivel de conciencia sobre seguridad de la información acorde a sus roles y responsabilidades.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Durante la contratación
CONTROL	7.2.2 Concienciación, educación y capacitación en seguridad de la información.		

DESARROLLO

Propósito: Capacitar a los empleados, contratistas y usuarios de terceros de la empresa dando un entrenamiento apropiado del conocimiento y de las actualizaciones regulares en políticas y procedimientos de la empresa, como sean relevantes para la

función de su trabajo.

Recomendación:
Capacitar al personal de forma apropiada sobre seguridad y el uso correcto de los sistemas de información y sus recursos, así como sobre la importancia dela seguridad en el tratamiento de los datos. Este proceso debiera comenzar en una inducción formal para introducir las políticas y expectativas de seguridad de la empresa antes de otorgar acceso a la información o servicios.

Se debe formar a todo el personal de la empresa que vaya a tratar datos del sistema de información sobre las normas de utilización, medidas de seguridad definidas, las instrucciones para tratar los recursos, la respuesta ante incidencias de seguridad que debe contemplar en el tratamiento de los datos, es una forma de disminuir los errores y los malos usos de los recursos y correcto desempeño de sus funciones.

Actividades:
- ✓ Capacitación permanente a todo el personal en materia de seguridad de la información.
- ✓ Incluir en la inducción a los nuevos empleados a través de charlas, las políticas de seguridad antes de otorgar acceso a la información o servicios.
- ✓ Informar a todos los empleados y contratistas a fin de que cumplan con las medidas establecidas por la empresa en el desempeño habitual de sus funciones.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Durante la contratación
CONTROL	7.2.3 Proceso disciplinario.		

DESARROLLO

Propósito: Definir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

Recomendación:
Seguir el proceso disciplinario formal contemplado en las normas que rigen al personal de la Administración Pública, para los empleados que violen la política, normas y procedimientos de seguridad de la empresa.

El proceso disciplinario contribuye como un elemento disuasivo para evitar que los empleados, contratistas y terceros violen las políticas y procedimientos de la seguridad y cualquier otro incumplimiento en la seguridad de la información.

Actividades: Establecer dentro del contrato una declaración de la obligación de dar cumplimiento sobre las políticas y procedimientos relativos a la seguridad de la información y que su incumplimiento deriva de las sanciones prescritas en la ley.

DOMINIO	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**OBJETIVO**	Cese o cambio de puesto de trabajo
CONTROL	7.3.1 Cese o cambio de puesto de trabajo.		

DESARROLLO

Propósito: Definir y asignar claramente las responsabilidades de realizar la desvinculación o cambio en las funciones

Recomendación: Documentar y comunicar las responsabilidades de terminación o cambio de puesto, estando claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado.

Informar de la obligación de mantener secreto profesional de los datos que conozca en desarrollo de sus funciones, a un después de finalizar la relación laboral que le une con la empresa, dicha responsabilidad debiera estar contenida en acuerdos de confidencialidad y en los términos y condiciones del empleo.

Actividades: Incluir dentro de los contratos las responsabilidades de acuerdo al tipo de información manejada por el funcionario, y las contenidas dentro de un contrato de confidencialidad, aún por un tiempo luego de la desvinculación.

DOMINIO	GESTIÓN DE ACTIVOS	**OBJETIVO**	Responsabilidad sobre los activos
CONTROL	8.1.1 Inventario de activos		

DESARROLLO

Propósito: Mantener actualizados, claramente identificados, confeccionando y

manteniendo un inventario de los activos más importantes de la empresa.

Recomendación: La empresa debe identificar todos los activos y documentarlos de acuerdo a su importancia, algunos de ellos son:

- **Información:** bases de datos, archivos de datos, documentación, contratos, acuerdos, documentación del sistema, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
- **Activos de software:** software de aplicaciones, software de sistemas, herramientas de protección, y utilidades.
- **Activos físicos:** equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos, personas, y sus calificaciones, habilidades y experiencia.
- **Activos intangibles**, tales como la reputación y la imagen de la empresa.

El 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 su valor comercial.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

Actividades:
Identificar todos los activos y elaborar y mantener actualizado un inventario de todos los activos importantes.

DOMINIO	GESTIÓN DE ACTIVOS	**OBJETIVO**	Responsabilidad sobre los activos
CONTROL	8.1.2 Propiedad de los activos		

DESARROLLO

Propósito: Mantener la protección adecuada de los activos de la empresa identificando los dueños para todos los activos y asignando la responsabilidad para el mantenimiento de los controles adecuados.

Recomendación: Designar los Propietarios de los activos identificados, para que puedan cumplir sus funciones de propietario. Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en la empresa.

Actividades:

- ✓ Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente en función a su valor.
- ✓ Definir y revisar periódicamente los requisitos de seguridad y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.
- ✓ Velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos.

DOMINIO	GESTIÓN DE ACTIVOS	**OBJETIVO**	Responsabilidad sobre los activos
CONTROL	8.1.3 Uso aceptable de los activos		

DESARROLLO

Propósito: identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Recomendación:
Los empleados, contratistas y terceros que usan o tienen acceso a los activos debieran estar al tanto de los límites existentes para el uso de la información y los activos asociados con los medios y recursos del procesamiento de la información; debieran ser responsables por el uso que le den a cualquier recurso de procesamiento de información realizado bajo su responsabilidad.

Utilizar una metodología para la clasificación de la información en función a cada uno de los pilares fundamentales de la seguridad de la misma. Confidencialidad, Integridad y Disponibilidad.

Todos los empleados, contratistas y usuarios de terceras partes debieran seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la misma.

Actividades: Se debe crear un procedimiento para el manejo y uso de los activos que incluyan:

- ✓ Reglas para la utilización de correo electrónico e internet.
- ✓ Medidas para sistemas de gestión y seguridad de la información.
- ✓ Lineamientos para el uso de dispositivos móviles.

DOMINIO	GESTIÓN DE ACTIVOS	**OBJETIVO**	Manejo de los soportes de almacenamiento
CONTROL	8.3.1 Gestión de soportes extraíbles		

DESARROLLO

Propósito: Establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la empresa.

Recomendación:
Se debieran considerar los siguientes lineamientos para la gestión de medios removibles:

- Si ya no son requeridos, los contenidos de los medios re-usables que no son removidos de la empresa no debieran ser recuperables.
- Se debieran establecer los procedimientos para identificar los ítems que podrían requerir de una eliminación segura.
- Muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipo y medios; se debe tener cuidado al seleccionar el contratista adecuado con los controles y la experiencia adecuados.
- Cuando sea posible se debiera registrar la eliminación de ítems confidenciales para mantener un rastro de auditoría.

Cuando se acumula medios para ser eliminados, se debiera tener en consideración el efecto de agregación, el cual puede causar que una gran cantidad de información no-confidencial se convierta en confidencial.

Actividades:

- ✓ Los contenidos de cualquier medio reutilizable, deben ser removidos de la empresa, haciéndolos irrecuperables.
- ✓ Todos los medios deben almacenarse en un ambiente seguro de acuerdo a las especificaciones del fabricante.
- ✓ La información almacenada en medios removibles que requiera estar disponible después del tiempo de vida del medio, debe ser almacenado en cualquier otro medio de tal manera que se garantice la permanencia de la información.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Requisitos de negocio para el control de accesos

CONTROL	9.1.1 Política de control de accesos.

DESARROLLO

Propósito: Establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de prestación de servicios de la empresa.

Recomendación: La política de seguridad debería tener en cuenta lo siguiente:

- Establecer criterios coherentes entre esta política de control de acceso y la política de clasificación de Información de los diferentes sistemas y redes que dispone la empresa.
- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones.
- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría depuestos de trabajo.
- Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.
- Aplicar revocación de los derechos de acceso.

Actividades:

- ✓ Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.
- ✓ Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas de información.
- ✓ Controlar la seguridad en la conexión entre la red de la empresa y otras redes públicas o privadas

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Requisitos de negocio para el control de accesos
CONTROL	9.1.2 Control de acceso a las redes y servicios asociados		

DESARROLLO

Propósito: Proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.

Recomendación: Los derechos de acceso a la red de los usuarios se deberían

mantener y actualizar según se requiera a través de la política de control de acceso.
La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de tablas o reglas predefinidas.

Actividades: Restringir la capacidad de conexión de los usuarios a través de Gateway de la red que filtran el tráfico por medio de tablas o reglas predefinidas. Los ejemplos de aplicaciones a las cuales se pueden aplicar las restricciones son:

- ✓ Mensajes; por ejemplo, correo electrónico.
- ✓ Transferencia de archivos.
- ✓ Acceso interactivo.
- ✓ Acceso a las aplicaciones.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	9.2.2 Gestión de los derechos de acceso asignados a usuarios		

DESARROLLO

Propósito: Establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Recomendación:
Un procedimiento formal para la gestión de derechos para otorgar y revocar el acceso debiera tener en cuenta:

- Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
- Verificar que el usuario tiene autorización para el uso del sistema, base de datos o servicio de información.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la política de seguridad.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se

desvincularon de la empresa o sufrieron la pérdida o robo de sus credenciales de acceso.

- Efectuar revisiones periódicas con el objeto de:
  - Cancelar identificadores y cuentas de usuario redundantes
  - Inhabilitar cuentas inactivas por un período de máximo de 60 días
  - Eliminar cuentas inactivas por un período mayor a 120 días
- Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

Actividades:
El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	9.2.3 Gestión de los derechos de acceso con privilegios especiales		

DESARROLLO

Propósito: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información. Se limitará y controlará la asignación y uso de privilegios.

Recomendación:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

Actividades:
El encargado del área de sistemas será el encargado de aprobar la asignación de

privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Gestión de acceso de usuario
CONTROL	9.2.5 Revisión de los derechos de acceso de los usuarios.		
DESARROLLO			
Propósito: Inspeccionar los derechos de acceso de los usuarios a intervalos regulares utilizando un procedimiento formal. **Recomendación:** • Revisar los derechos de acceso de los usuarios a intervalos de 4 a 6 meses y cuando haya cualquier cambio, asenso, cambio de puesto, terminación del contrato. • Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses aproximadamente • Revisar las asignaciones de privilegios a intervalos de en periodos no mayor a6 meses, a fin de garantizar que no se obtengan privilegios no autorizados. • Registrar los cambios en las cuentas privilegiadas para una revisión periódica. **Actividades:** Revisar regularmente los derechos de acceso de los usuarios para mantener un control efectivo sobre el acceso a la data y los servicios de información de la empresa.			

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Control de acceso a sistemas y aplicaciones
CONTROL	9.4.1 Restricción del acceso a la información		
DESARROLLO			

Propósito: Restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

Recomendación:
Se debiera considerar controles para reforzar los requerimientos de restricción del acceso:

- Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El encargado de la información involucrada será responsable de la adjudicación de accesos a las funciones.
- Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder.
- Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

Actividades:

- ✓ Limitar y controlar la asignación y uso de privilegios.
- ✓ Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- ✓ Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para el rol funcional de cada empleado.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Control de acceso a sistemas y aplicaciones
CONTROL	9.4.2 Procedimientos seguros de inicio de sesión		
DESARROLLO			
Propósito: controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de Login			

Recomendación: El procedimiento de registro en un sistema u aplicación debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado.

Actividades: Diseñar un registro que cumpla con los siguientes aspectos:

- ✓ No debe mostrárselos identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro.
- ✓ Mostar la advertencia general que a la computadora sólo pueden tener acceso los usuarios autorizados.
- ✓ Proporcionar mensajes de ayuda durante el procedimiento de registro que ayuden al usuario no-autorizado.
- ✓ Limitar el número de intentos de registro infructuosos permitidos; por ejemplo, tres intentos.
- ✓ Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro. Si se excede este tiempo, el sistema debería terminar el registro.
- ✓ Mostrar información al término de un registro satisfactorio
- ✓ Mostrar la clave secreta que se está ingresando o considerar esconder los caracteres de la clave secreta mediante símbolos.
- ✓ No deben transmitirse claves secretas en un texto abierto a través de la red.

DOMINIO	CONTROL DE ACCESOS	**OBJETIVO**	Control de acceso a sistemas y aplicaciones
CONTROL	9.4.3 Gestión de contraseñas de usuario.		

DESARROLLO

Propósito: Asignar contraseñas y se controlará a través de un proceso de administración formal

Recomendación:

- Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad
- Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo deben

suministrarse una vez acreditada la identidad del usuario.
- Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- Configurar los sistemas de tal manera que:
  - Las contraseñas sean del tipo “password fuerte” y tengan mínimo 8caracteres entre ellos alfanuméricos mayúsculas, minúsculas y especiales.
  - Suspender o bloquear permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta. En caso de bloqueo debe pedirla rehabilitación ante quien corresponda.
  - Solicitar el cambio de la contraseña cada 30 a 45 días
  - Impedir que las últimas 10 a 12 contraseñas sean reutilizadas.

Actividades:
- ✓ Verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de información
- ✓ Monitorear periódicamente el cambio de contraseñas de usuario

DOMINIO	CIFRADO	**OBJETIVO**	Controles criptográficos
CONTROL	10.1.1 Política de uso de los controles criptográficos.		

DESARROLLO

Propósito: Desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información de la empresa.

Recomendación: Implementar controles criptográficos en las políticas de seguridad de los sistemas de información para la protección de claves de acceso, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la empresa.
Se pueden utilizar controles criptográficos para lograr diferentes objetivos de seguridad:
- **Confidencialidad:** utilizando la codificación de la información para proteger la información confidencial o crítica, ya sea almacenada o transmitida;
- **Integridad/autenticidad:** utilizando firmas digitales o códigos de autenticación del mensaje para proteger la autenticidad e integridad de la información confidencial o crítica almacenada o transmitida;
- **No-repudiación:** utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

Actividades:

- ✓ Diseñar e implementar controles criptográficos**.**
- ✓ Protección de claves de acceso a sistemas, datos y servicios.
- ✓ Transmisión de información clasificada, fuera del ámbito de la empresa.

DOMINIO	CIFRADO	**OBJETIVO**	Controles criptográficos
CONTROL	10.1.2 Gestión de claves		

DESARROLLO

Propósito: Establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la empresa.

Recomendación: Todas las claves criptográficas deben estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no-autorizada.
Se debe proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.

Actividades:
El sistema de gestión de claves se debe basar en un conjunto de estándares, procedimientos y métodos seguros acordados para:

- ✓ Generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones.
- ✓ Generar y obtener certificados de claves públicas.
- ✓ Distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas.
- ✓ Almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves; cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debe cambiar las claves y cómo se realiza esto.
- ✓ Lidiar con las claves comprometidas.
- ✓ Revocar las claves incluyendo cómo se debe retirar o desactivar las claves; por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la empresa (en cuyos casos las claves también deben ser archivadas).
- ✓ Recuperar las claves cuando han sido pérdidas o corrompidas como parte de la continuidad y gestión del negocio; por ejemplo, para recuperar la información codificada.
- ✓ Archivar las claves; por ejemplo, para la información archivada o respaldada.
- ✓ Destruir las claves.

- ✓ Registrar y auditar las actividades relacionadas con la gestión de claves.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Áreas seguras
CONTROL	11.1.1 Perímetro de seguridad física		

DESARROLLO

Propósito: Utilizar los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) para proteger las áreas que contengan información y recursos para su procesamiento.

Recomendación:

- Los perímetros de seguridad deben estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo.
- Los perímetros del área que contienen los medios de procesamiento de información deben ser físicamente sólidos, es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado.
- Las paredes externas del local deben ser una construcción sólida y todas las puertas externas deben estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control.
- Las puertas y ventanas deben quedar aseguradas cuando están desatendidas y considerar una protección externa para las ventas.
- Se debe operar en concordancia con el código contra-incendios local de una manera totalmente segura.
- Las áreas no ocupadas deben contar con alarma en todo momento.
- Proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones.
- Los medios de procesamiento de información manejados por la empresa deben estar físicamente separados de aquellas manejadas por terceros.

Actividades:

- ✓ Definir y documentar claramente los perímetros de seguridad de acuerdo a la ubicación y requerimientos de seguridad de los activos.
- ✓ Ubicar las instalaciones de procesamiento de información dentro del perímetro del área de construcción físicamente sólida.

- ✓ Instalar alarmas a las puertas de emergencia en un perímetro de seguridad.
- ✓ Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
- ✓ El Responsable de Seguridad de la Información debe llevar un registro actualizado de los sitios protegidos, indicando:
  a) Identificación del Área.
  b) Principales elementos a proteger.
  c) Medidas de protección física.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Áreas seguras
CONTROL	11.1.2 Controles físicos de entrada		

DESARROLLO

Propósito: Proteger las áreas seguras mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Recomendación:

- La fecha y la hora de entrada y salida de los visitantes debe ser registrada y todos los visitantes deben ser supervisados a no ser que su acceso haya sido previamente aprobado.
- Sólo se le debe permitir acceso por propósitos específicos y autorizados a visitantes y se deben emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.
- El acceso a áreas donde se procesa o almacena información sensible debe ser controlada y restringida sólo al personal autorizado.
- Para todos los usuarios empleados, contratistas y terceras personas y todos los visitantes deben usar como requisito alguna forma de identificación visible.
- Al personal de servicio de apoyo de terceros se le debe otorgar acceso restringido las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debe ser autorizado y monitoreado.
- Los derechos de acceso a áreas seguras deben ser revisados y actualizados regularmente, y revocados cuando sea necesario.

Actividades:

- ✓ Establecer requerimientos de seguridad del área y los procedimientos de emergencia, para autorizar e instruir al visitante en el momento que se le

permita el ingreso.
- ✓ Supervisar o inspeccionar a los visitantes en áreas protegidas.
- ✓ Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
- ✓ Diseñar controles de autenticación para autorizar y validar todos los accesos.
- ✓ Implementar el uso de una identificación unívoca visible para todo el personal del área protegida.
- ✓ Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Áreas seguras
CONTROL	11.1.3 Seguridad de oficinas, despachos e instalaciones		

DESARROLLO

Propósito: Debiera diseñar y aplicar la seguridad física para las oficinas, despachos e instalaciones.

Recomendación:

- Se debe tener en cuenta los estándares y regulaciones de sanidad y seguridad relevantes;
- Se debe localizar los medios claves para evitar el acceso del público.
- El área de procesamiento de información relevante debe ser discreta y dar una indicación mínima de su propósito, sin carteles obvios dentro y fuera del área que indiquen la presencia de actividades de procesamiento de información.
- Los directorios y teléfonos internos que identifiquen la ubicación de los medios de procesamiento de la información no debieran estar accesibles al público.
- Las instalaciones críticas deben situarse evitando el acceso al público
- Debe existir un estándar para la elección de contraseñas robustas.

Actividades:

- ✓ Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- ✓ Establecer que el área donde se realicen actividades de procesamiento de información sean discretas y solo se muestre un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- ✓ Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida

para evitar solicitudes de acceso, el cual podría comprometer la información.
- ✓ Establecer que las puertas y ventanas cerradas cuando no haya vigilancia tengan protección.
- ✓ Implementar una lista de lugares seguros para almacenar los materiales peligrosos combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas de la empresa.
- ✓ Ubicar un sitio seguro y distante del lugar de procesamiento para almacenar los equipos redundantes y la información de resguardo (backup).

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Áreas seguras
CONTROL	11.1.4 Protección contra las amenazas externas y ambientales		

DESARROLLO

Propósito: Asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Recomendación: Se deben considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

- Los suministros a granel como papelería no debiera almacenarse en el área asegurada.
- El equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal.
- Proporcionar equipo contra-incendios ubicado adecuadamente.

Actividades

- ✓ Instalar a una distancia adecuada y en un área segura el equipamiento de contingencia, que permita evitar el daño frente a un desastre que afecte al sitio principal.
- ✓ Mantener en un lugar visible y de rápido acceso el equipamiento de extinción de incendios.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Áreas seguras

CONTROL	11.1.5 El trabajo en áreas seguras.

DESARROLLO

Propósito: Diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

Recomendación: Para incrementar la seguridad en las áreas protegidas se debe tener en cuenta:

- El personal debe estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer.
- Evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos.
- Las áreas aseguradas vacías deben ser cerradas físicamente bajo llave y revisadas periódicamente.
- No se debe permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado.

Actividades:

- ✓ Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
- ✓ Evitar la ejecución de trabajos por parte de terceros sin supervisión.
- ✓ Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
- ✓ Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas a las instalaciones de procesamiento de información sensible.
- ✓ Mantener un registro de todos los accesos de personas ajenas.
- ✓ Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el responsable de dicho área o el responsable del área Informática y el responsable de seguridad de la información.
- ✓ Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Seguridad de los equipos.
CONTROL	11.2.1 Emplazamiento y protección de equipos.		

DESARROLLO

Propósito: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la empresa. Proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.

Recomendación:

- Ubicar el equipo de manera que se minimice el acceso innecesario a las áreas de trabajo.
- Los medios de procesamiento de la información que manejan data confidencial deben ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso.
- Asegurar los medios de almacenaje para evitar el acceso no autorizado.
- Aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida.
- Adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo.
- Establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información.
- Monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.
- Aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.
- Proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

Actividades:

- ✓ Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
- ✓ Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Seguridad de los equipos.
CONTROL	11.2.4 Mantenimiento de los equipos		

DESARROLLO

Propósito: Mantener correctamente los equipos para asegurar su continua disponibilidad e integridad.

Recomendación:

- El equipo se debe mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor.
- Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo.
- Mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo.
- Implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la empresa; cuando sea necesario y revisar la información confidencial del equipo, o se debiera verificar al personal de mantenimiento.
- Cumplir con todos los requerimientos impuestos por las pólizas de seguros.

Actividades:

- ✓ Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área.
- ✓ Llevar un registro actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- ✓ Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- ✓ Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- ✓ Registrar el retiro de equipamiento de las sedes de la empresa para su mantenimiento.
- ✓ Eliminar la información confidencial que contenga cualquier equipamiento, realizándose previamente las respectivas copias de resguardo antes de que se vallan a llevar el equipo para hacer mantenimiento.

DOMINIO	SEGURIDAD FÍSICA Y AMBIENTAL.	**OBJETIVO**	Seguridad de los equipos.
CONTROL	11.2.5 Salida de activos fuera de las dependencias de la empresa		
DESARROLLO			

Propósito: Los equipos, información o software no deben retirarse sin autorización previa.

Recomendación:

- No se debe retirar equipo, información o software sin autorización previa.
- Los usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del área deben estar claramente identificados.
- Establecer límites de tiempo para el retiro del equipo y se debe realizar un chequeo de la devolución.
- Cuando sea necesario y apropiado, el equipo debe ser registrado como retirado del área y se debe registrar su retorno.

Actividades:

- ✓ Especificar un tiempo máximo para el equipamiento retirado y verificarse el cumplimiento de retorno.
- ✓ Llevar un registro de entrada y salida de los equipos de la dependencia.

DOMINIO	SEGURIDAD EN LA OPERATIVA	**OBJETIVO**	Responsabilidades y procedimientos de operación
CONTROL	12.1.1 Documentación de procedimientos de operación.		

DESARROLLO

Propósito: Documentar, mantener y poner a disposición los procedimientos de operación de todos los usuarios, a quien lo necesite.

Recomendación:

- Documentar 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.
- Los procedimientos de operación deben especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:
  - Procesamiento y manejo de información.
  - Copia de seguridad o respaldo.
  - Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y

últimos trabajos.
- Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
- Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
- Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema;
- La gestión de la información del rastro de auditoría y registro del sistema.

Los procedimientos de operación y los procedimientos documentados para las actividades del sistema deben ser tratados como documentos formales y cambios autorizados por la gerencia. Donde sea técnicamente factible, los sistemas de información deben ser manejados consistentemente, utilizando los mismos procedimientos, herramientas y utilidades.

Actividades:

- ✓ Documentar y mantener actualizados los procedimientos operativos identificados y sus cambios serán autorizados por el Responsable de Seguridad de la Información.
- ✓ Diseñar y establecer procedimientos para la operación de la infraestructura critica de las TIC'C que incluya:
  - Manejo y procedimiento de la información.
  - Respaldos.
  - Requerimientos de tareas automatizadas, incluyendo las dependencias con otros sistemas. Alertas sobre tareas ejecutadas correcta e incorrectamente.
  - Instrucciones para manejar errores o condiciones excepcionales.
- ✓ Preparar adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:
  - Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
  - Instalación y mantenimiento de las plataformas de procesamiento.
  - Monitoreo del procesamiento y las comunicaciones.
  - Inicio y finalización de la ejecución de los sistemas.
  - Programación y ejecución de procesos.
  - Gestión de servicios.
  - Resguardo de información.
  - Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
  - Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
  - Uso del correo electrónico.

DOMINIO	SEGURIDAD EN LA OPERATIVA	**OBJETIVO**	Responsabilidades y procedimientos de operación
CONTROL	12.1.2 Gestión de cambios.		

DESARROLLO

Propósito: Controlar los cambios en los medios y sistemas de procesamiento de la información.

Recomendación:
Los sistemas operacionales y el software de aplicación deben estar sujetos a un estricto control gerencial del cambio.
El control inadecuado de los cambios en los medios de procesamiento de la información y los sistemas es una causa común de fallas en el sistema o en la seguridad. Los cambios en los sistemas de operación sólo se deben realizar cuando existe una razón comercial válida para hacerlo, como un incremento en el riesgo para el sistema.
Los cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la etapa operacional, pueden influir en la confiabilidad de la aplicación.

Actividades:
- ✓ Establecer las responsabilidades y procedimientos formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos.
- ✓ Mantener un registro de auditoría que contenga toda la información relevante de cada cambio.
- ✓ El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, además debe evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

DOMINIO	SEGURIDAD EN LA OPERATIVA	**OBJETIVO**	Protección contra código malicioso
CONTROL	12.2.1 Controles contra el código malicioso.		

DESARROLLO

Propósito: Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se debieran implementar procedimientos para el apropiado conocimiento del usuario.

Recomendación: El Responsable de Seguridad de la Información debe definir controles de detección y prevención para la protección contra software malicioso y concientizar a los usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles. Se deberá considerar los siguientes lineamientos:

- Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
- Realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos críticos; se deberá investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas.
- Se puede instalar software para protegerse de códigos maliciosos para proporcionar actualizaciones automáticas de archivos de definición y motores de lectura para asegurarse que la protección esté actualizada. Además, este software se puede instalar en cada desktop para que realice chequeos automáticos.

Actividades:

- ✓ Establecer una política formal que prohíba el uso no autorizado de software.
- ✓ Establecer una política formal que proteja ante los riesgos asociados al obtener software y archivos a través de redes externas, o cualquier otro medio, indicando que medidas preventivas deber ser tomadas.
- ✓ Efectuar revisiones periódicas del software y los contenidos de los datos de los sistemas que soportan procesos de negocio críticos, y se debe investigar ante la presencia de cualquier archivo no autorizado.
- ✓ Se debe instalar software que detecte código malicioso que sea enviado a través de cualquier medio y este debe ser actualizado regularmente.
- ✓ Definir procedimientos y responsabilidades para tratar con código malicioso, entrenamiento en el uso, reporte recuperación ante ataques.
- ✓ Preparar apropiados planes de continuidad del negocio para recuperarse ante eventuales ataques.
- ✓ Implementar procedimientos para recopilar regularmente información como listas de correo o sitios informativos.

DOMINIO	SEGURIDAD EN LA OPERATIVA	**OBJETIVO**	Copias de seguridad
CONTROL	12.3.1 Copias de seguridad de la información.		

DESARROLLO

Propósito: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Recomendación: 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:
Se debieran considerar los siguientes ítems para el respaldo de la información:

- Definir el nivel necesario de respaldo de la información.
- Se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.
- La frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la empresa, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la misma.
- Las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal.
- A la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo.
- Los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia.
- Los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.
- En situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

Los procedimientos de respaldo pueden ser automatizados para facilitar el proceso de respaldo y restauración. Estas soluciones automatizadas debieran ser probadas suficientemente antes de su implementación y también a intervalos regulares.

Actividades:

- ✓ Proveer registros completos y registros de la información que se respalda, así también como los procedimientos de recuperación.

- ✓ Probar regularmente los medios de recuperación para asegurar que puedan ser utilizados.
- ✓ Los procedimientos de restauración deben ser probados regularmente.

DOMINIO	SEGURIDAD EN LA OPERATIVA	**OBJETIVO**	Consideraciones de las auditorías de los sistemas de información.
CONTROL	12.7.1 Controles de auditoría de los sistemas de información.		

DESARROLLO

Propósito: Planificar y acordar cuidadosamente los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos para minimizar el riesgo de interrupciones de los procesos de la empresa.

Recomendación:
Se pueden tener presente los siguientes lineamientos:

- Los requisitos de auditoría se deberían acordaron la dirección correspondiente.
- Acordar y controlar el alcance de las verificaciones.
- Las verificaciones se deberían limitar al acceso de solo lectura del software y los datos.
- El acceso diferente al de solo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría.
- Documentar todos los procedimientos, requisitos y responsabilidades.
- La persona que realiza la auditoría debería ser independiente de las actividades auditadas.

Actividades:

- ✓ Acordar los requerimientos de auditoría con la autoridad.
- ✓ Acordar y controlar el alcance de los chequeos.
- ✓ Los chequeos deben limitarse a un acceso de “sólo lectura” al software y los datos.
- ✓ Identificar explícitamente y disponer los recursos para realizar los chequeos.
- ✓ Monitorear y registrar todos los accesos para producir un histórico de referencia; considerar rastros de referencia con impresión horaria para los datos o sistemas críticos.
- ✓ Documentar todos los procedimientos, requerimientos y responsabilidades.

DOMINIO	SEGURIDAD EN LAS TELECOMUNICACIONES.	**OBJETIVO**	Gestión de la seguridad en las redes
CONTROL	13.1.1 Controles de red.		

DESARROLLO

Propósito: Manejar y controlar las redes con el fin de proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Recomendación: El Responsable de Seguridad de la Información debiera implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se debieran considerar los siguientes ítems:

- Cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo.
- Se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario.
- Se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados; también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y las computadoras conectadas.
- Se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes.
- Las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio de la empresa y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.

Actividades:

- ✓ Separar la responsabilidad en la operación de las redes de las responsabilidades en el manejo de los servidores.
- ✓ Establecer responsabilidades y procedimientos de administración de

equipamiento remoto.
- ✓ Establecer controles especiales para resguardar la confidencialidad e integridad de los datos que viajan sobre redes públicas o inalámbricas.
- ✓ Establecer los mecanismos apropiados de monitoreo y registro de las acciones relevantes para la seguridad.

DOMINIO	SEGURIDAD EN LAS TELECOMUNICACIONES.	**OBJETIVO**	Gestión de la seguridad en las redes
CONTROL	13.1.2 Mecanismos de seguridad asociados a servicios en red.		

DESARROLLO

Propósito: Identificar e incluir las en el contrato de redes las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Recomendación: Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde una simple banda ancha manejada ofertas complejas de valor agregado.
Las características de seguridad de los servicios de red pueden ser:

- la tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red.
- parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red.
- cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones.

De acuerdo a lo anterior, se debiera determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debiera acordar el derecho de auditoría.
Se debieran identificar los acuerdos de seguridad necesarios para servicios particulares; como las características de seguridad, niveles de servicio y requerimientos de gestión.
La empresa se debiera asegurar que los proveedores de servicio de red implementen estas medidas.

Actividades:

- ✓ Aplicar tecnología para asegurar los servicios de red, tal como autenticación,

encriptación y control de conexiones.
- ✓ Establecer conexiones seguras a través de reglas de accedo de acuerdo los requerimientos de la empresa.

DOMINIO	SEGURIDAD EN LAS TELECOMUNICACIONES.	**OBJETIVO**	Gestión de la seguridad en las redes
CONTROL	13.1.3 Segregación de redes		

DESARROLLO

Propósito: Reducir las oportunidades de una modificación no-autorizada, no intencional o mal uso de los activos de la empresa.

Recomendación:
- Tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección.
- Separar la iniciación de un evento de su autorización.
- Considerar la posibilidad de colusión en el diseño de los controles.
- Es importante que la auditoría de seguridad se mantenga independiente.

Actividades:
- ✓ Crear perfiles de usuario que sean consecuentes con las descripciones del cargo que desempeñen y que contengan los mínimos acceso a los sistemas de la información para llevar a cabo sus funciones.
- ✓ El encargado de seguridad debe validar estos perfiles y auditarlos cada 6 meses.
- ✓ Separar la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.
- ✓ Implementar controles que incluya:
  - Monitoreo de las actividades.
  - Registros de auditoría y control periódico de los mismos.
  - Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

DOMINIO	SEGURIDAD EN LAS TELECOMUNICACIONES.	**OBJETIVO**	Intercambio de información con partes externas
CONTROL	13.2.3 Mensajería electrónica.		

DESARROLLO

Propósito: Proteger adecuadamente la información involucrada en mensajes electrónicos.

Recomendación: Los mensajes electrónicos como el correo electrónico, Intercambio Electrónico de Data (EDI), y los mensaje instantáneos representa un papel cada vez más importante en las comunicaciones comerciales. Los mensajes electrónicos tienen riesgos diferentes que las comunicaciones basadas en papel.
Las consideraciones de seguridad para los mensajes electrónicos incluyen lo siguiente:

- Proteger los mensajes del acceso no-autorizado, modificación o negación del servicio.
- Asegurar la correcta dirección y transporte del mensaje.
- Confiabilidad y disponibilidad general del servicio.
- Consideraciones legales, por ejemplo los requerimientos para firmas electrónicas.
- Obtener la aprobación antes de utilizar los servicios públicos externos como un
- mensaje instantáneo o intercambio de archivos.
- Niveles mayores de autenticación controlando el acceso de las redes de acceso público.

Actividades:

- ✓ Proteger los mensajes del acceso no-autorizado, modificación o negación del servicio.
- ✓ Asegurarla correcta asignación de la dirección y el transporte del mensaje.
- ✓ Niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.
- ✓ Obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos.

DOMINIO	SEGURIDAD EN LAS TELECOMUNICACIONES.	**OBJETIVO**	Intercambio de información con partes externas

CONTROL	13.2.4 Acuerdos de confidencial y secreto

DESARROLLO

Propósito: Identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la empresa para proteger la información.

Recomendación: Definir, implementar y revisar regularmente los acuerdos de confidencialidad o de no-divulgación para la protección de la información de la E.S.E Hospital Regional Centro. Además, cumplir con toda legislación o normativa que cobije a la empresa en materia de confidencialidad de la información.
Dichos acuerdos deben celebrarse tanto con el personal de la empresa como con aquellos terceros que se relacionen de alguna manera con la información.

Actividades:

- ✓ Clasificación de la información (pública-secreta).
- ✓ Definición de la duración del acuerdo, incluyendo la duración indefinida.
- ✓ Estipulación de las acciones necesarias una vez que el acuerdo haya terminado.
- ✓ Asignación de responsabilidades para evitar la divulgación no-autorizada de la información.
- ✓ Describir el derecho de auditar y supervisar actividades que involucren información secreta.
- ✓ Estipular el procedimiento a seguir frente a una divulgación no autorizada o violaciones de la información secreta.
- ✓ Definición de los términos de devolución o destrucción de la información, una vez finaliza un acuerdo.
- ✓ Describir las acciones necesarias en el caso de no cumplir con el acuerdo.

DOMINIO	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	**OBJETIVO**	Requisitos de seguridad de los sistemas de información.
CONTROL	14.1.1 Análisis y especificación de los requisitos de seguridad		

DESARROLLO

Propósito: Especificar los requisitos para los controles de seguridad en las declaraciones sobre los requisitos de la empresa para nuevos sistemas de información o mejoras a los sistemas con los que ya cuenta la empresa.

Recomendación: Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.
Si se adquieren nuevos productos, se debe seguir un proceso formal de adquisición y prueba. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Actividades:

- ✓ Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados.
- ✓ Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.
- ✓ Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

DOMINIO	RELACIONES CON SUMINISTRADORES.	**OBJETIVO**	Seguridad de la información en las relaciones
CONTROL	15.1.1 Política de seguridad de la información para suministradores		

DESARROLLO

Propósito: acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la empresa con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.

Recomendación: el tratamiento de la seguridad de los activos debe considerar los siguientes controles antes de proporcionar a los clientes acceso a cualquier activo de la empresa:

- Cumplimiento de la Política de seguridad de la información de la empresa.
- Protección de activos del organismo, incluyendo:
  - Procedimientos para proteger los bienes de la empresa, abarcando los activos físicos, la información y el software.
  - Procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data.
  - Controles para proteger y garantizar integridad de la información.
  - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo
  - Restricciones sobre el copiado y divulgación de información.
- Las respectivas obligaciones de la empresa y el suministrador
- Responsabilidades legales, contractuales y derechos de propiedad intelectual (IPRs).

Los requerimientos de seguridad relacionados con el acceso del suministrador a los activos de la empresa pueden variar considerablemente dependiendo de los medios de procesamiento de la información y la información a la cual se tiene acceso.

Actividades

- ✓ Realizar acuerdos con el proveedor, los cuales contengan todos los riesgos identificados y los requerimientos de seguridad.
- ✓ Establecer un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- ✓ Llevar un Proceso claro y detallado de administración de cambios.
- ✓ Diseñar Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- ✓ Diseñar Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- ✓ Diseñar Controles que garanticen la protección contra software malicioso.

DOMINIO	RELACIONES CON SUMINISTRADORES.	**OBJETIVO**	Seguridad de la información en las relaciones
CONTROL	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.		
DESARROLLO			
Propósito: establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la empresa.			

Recomendación: Dentro del contrato o acuerdo se debe considerar los siguientes términos a incluirse en el acuerdo para cumplir con los requerimientos de seguridad:

- La política de seguridad de la información.
- Capacitación del usuario y administrador en métodos, procedimientos y seguridad.
- Asegurar la conciencia del usuario para las responsabilidades y problemas de la seguridad de la información.
- Provisión para la transferencia de personal, cuando sea apropiado.
- Responsabilidades relacionadas con la instalación y mantenimiento de hardware y software.
- Una estructura de reporte clara y formatos de reporte acordados.
- Un proceso claro y especificado de gestión de cambio.
- Una definición del criterio del desempeño verificable, su monitoreo y reporte.
- El derecho a monitoreo o seguimiento y a revocar, cualquier actividad relacionada con los activos de información del servicio.
- Política de control de acceso, abarcando.
  - Las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros.
  - Métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas.
  - Un proceso de autorización para el acceso y privilegios del usuario.
  - Un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso.
  - Un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado.
  - Un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas.
- El derecho de auditar las responsabilidades definidas en el acuerdo, el derecho que un tercero lleve a cabo la auditoria, y enumerar los derechos estatutarios de los auditores.
- Requerimientos de continuidad del negocio, incluyendo las medidas de disponibilidad y confiabilidad, en concordancia con las prioridades comerciales de la empresa.
- Las obligaciones respectivas de la empresa y el proveedor.
- Acuerdos para el manejo de incidentes de seguridad.
- Requerimientos de continuidad.

Actividades:

- ✓ Organizar, planear y manejar la transición a un acuerdo de abastecimiento externo que cuente con los procesos adecuados para manejar los cambios y los acuerdos de negociación/terminación.
- ✓ Definir el acuerdo o contrato donde se considere procedimientos para continuar el procesamiento en el evento que la tercera persona no pueda suministrar los servicios para evitar cualquier demora en acordar el reemplazo de los servicios.

DOMINIO	RELACIONES CON SUMINISTRADORES.	**OBJETIVO**	Gestión de la prestación del servicio por suministradores
CONTROL	15.2.1 Supervisión y revisión de los servicios prestados por terceros.		

DESARROLLO

Propósito: Monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.

Recomendación: El monitoreo y revisión de los servicios de terceros deberá 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. Esto debiera involucrar una relación y proceso de gestión de servicio entre la empresa y la tercera persona para:

- Monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos.
- Revisar los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme lo requieran los acuerdos.
- Proporcionar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la empresa conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte.
- Revisar los rastros de auditoría de terceros y los registros de eventos de seguridad,
- problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado.
- Resolver y manejar cualquier problema identificado.

La empresa debe mantener el control y la visibilidad general suficiente en todos los aspectos de seguridad con relación a la información confidencial o crítica o los medios de procesamiento de la información que la tercera persona ingresa, procesa o maneja. La empresa debe asegurarse de mantener visibilidad en las actividades de seguridad como la gestión del cambio, identificación de vulnerabilidades y reporte/respuesta de un incidente desagradada través de un proceso, formato y estructura de reporte definidos. En caso de abastecimiento externo, la empresa necesita estar al tanto que la responsabilidad final de la información procesada por un proveedor externo se mantenga en la empresa.

Actividades:

- ✓ Monitorear los niveles de servicio y chequear su adherencia a los acuerdos.
- ✓ Revisar los reportes generados por los terceros y acordar reuniones.
- ✓ Suministrar información ante incidentes de seguridad de manera de dar cumplimiento a la normativa de seguridad.
- ✓ Revisar los registros de auditoría de los terceros, frente a problemas de seguridad, operacionales, fallas y discontinuidad del servicio.
- ✓ Resolver los problemas identificados.

Estructura del documento:

Posibles formatos donde se puede mantener control y visibilidad general sobre:

Formato de registro la Gestión del Cambio

FECHA (D/M/AA)	DEPENDENCIA /ORIGEN DEL ERROR	CODIGO /TIPO DE ERROR	DESCRIPCION DEL ERROR	CAUSAS	PROCEDIMIENTO REALIZADO	RESPONSABLE
_ _ _	_ _ _ _ _ _	_ _ _	_ _ _ _ _ _	_ _ _	_ _ _ _ _ _ _	_ _ _ _ _ _
_ _ _	_ _ _ _ _ _	_ _ _	_ _ _ _ _ _	_ _ _	_ _ _ _ _ _ _	_ _ _ _ _ _

Matriz de Riesgos

ID	RIESGO	POSIBLE RESULTADO	SINTOMA	PROBABILIDAD	IMPACTO	PRIORIDAD	RESPUESTA	RESPONSABLE
_ _ _	_ _ _	_ _ _ _	_ _ _	_ _ _	_ _ _	_ _ _	_ _ _	_ _ _
_ _ _	_ _ _	_ _ _ _	_ _ _	_ _ _	_ _ _	_ _ _	_ _ _	_ _ _

- **ID:** Un código o número identificador del riesgo.
- **Riesgo:** Descripción detallada del riesgo.
- **Posible resultado:** Descripción específica sobre cuál sería el efecto del riesgo en caso de que este ocurra.
- **Síntoma:** Identifica y describe una señal de alarma o advertencia de que el riesgo puede ocurrir. Es importante mencionar que no todos los riesgos tienen síntomas.
- **Probabilidad:** Evalúa la probabilidad de que el riesgo suceda. Esta probabilidad puede ser alta, media o baja dependiendo del riesgo.
- **Impacto:** Evalúa el grado de impacto en caso de que el riesgo ocurra. Este impacto puede ser alto, medio o bajo dependiendo del riesgo en sí mismo.
- **Prioridad:** Prioriza los riesgos en una escala de 1 al 9, 1 indica el nivel máximo

crítico y 9 el nivel mínimo.

- **Respuestas:** Especifica la acción (control) que el equipo llevará a cabo para eliminar, trasladar o mitigar el riesgo.
- **Responsable:** Nombre o rol del responsable de llevar a cabo la acción de respuesta al riesgo.

DOMINIO	RELACIONES CON SUMINISTRADORES.	**OBJETIVO**	Gestión de la prestación del servicio por suministradores.
CONTROL	15.2.2 Gestión de cambios en los servicios prestados por terceros.		

DESARROLLO

Propósito: administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos.

Recomendación: Se debe considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.

El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta:
1. Los cambios realizados por la empresa para implementar:
   - Aumento los servicios ofrecidos actualmente.
   - Desarrollo de cualquier aplicación y sistema nuevo.
   - Modificaciones o actualizaciones de las políticas y procedimientos de la empresa.
   - Controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad.
2. Cambios en los servicios de terceros para implementar:
   - Cambios y mejoras en las redes.
   - Uso de tecnologías nuevas.
   - Adopción de productos nuevos o versiones más modernas.
   - Desarrollo de herramientas y ambientes nuevos.
   - Cambios en la ubicación física de los medios del servicio.
   - Cambio de vendedores.

Actividades:
El proceso de administración de cambios, necesita manejar:

- ✓ Los cambios realizados por la empresa para implementar mejoras a los servicios ofrecidos, desarrollo aplicaciones; modificaciones o actualizaciones de los procedimientos o políticas de la empresa; nuevos controles que resuelvan

incidentes de seguridad.

- ✓ Los cambios realizados por los terceros para mejorar las redes, el uso de nuevas tecnologías, adopción de nuevos productos o nuevas versiones, nuevas herramientas de desarrollo y ambientes, cambios a las locaciones físicas o facilidades de servicio, cambios en los fabricantes.

DOMINIO	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	16.1.1 Responsabilidades y procedimientos		

DESARROLLO

Propósito: establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Recomendación:

- Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:
  - Fallas operativas
  - Código malicioso
  - Intrusiones
  - Fraude informático
  - Error humano
  - Catástrofes naturales.
- Registrar pistas de auditoría y evidencia similar para:
  - Análisis de problemas internos.
  - Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
  - Negociación de compensaciones por parte de los proveedores de software y de servicios.
- Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.
- Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
  - Definición de las primeras medidas a implementar
  - Análisis e identificación de la causa del incidente.
  - Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.

- Comunicación formal con las personas afectadas o involucradas con la recuperación, del incidente.
- Notificación de la acción a la autoridad y/o entidades pertinentes.

- Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
  - Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
  - Documentación de todas las acciones de emergencia emprendidas en forma detallada.
  - Comunicación de las acciones de emergencia.
  - Constatación.

Actividades: Establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

DOMINIO	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	16.1.2 Notificación de los eventos de seguridad de la información.		

DESARROLLO

Propósito: Reportar los eventos de seguridad de la información a través de los canales gerenciales apropiados lo más rápidamente posible.

Recomendación: establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes, estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información.
Establecer un punto de contacto para el reporte de eventos en la seguridad de la información, asegurándose que este punto de contacto sea conocido a través de toda la empresa, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.
Todos los usuarios empleados, contratistas y terceros debieran estar al tanto de la responsabilidad de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. También debieran estar al tanto del procedimiento para reportar eventos en la seguridad de la información y el punto de contacto. Los procedimientos de reporte debieran incluir:

- Procesos de retroalimentación adecuados para asegurar que aquellos que

reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema.

- Formatos donde se reporte los eventos en la seguridad de la información para respaldarla acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información.
- Se debiera tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir:
  1. Anotar todos los detalles importantes inmediatamente (por ejemplo, el tipo de no cumplimiento o violación, mal funcionamiento actual, mensajes en la pantalla, conducta extraña).
  2. No llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto.
- Referenciar un proceso disciplinario formal establecido para tratar con los usuarios empleados, contratistas o terceros que cometen violaciones de seguridad.

Actividades:

- ✓ Establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de notificación de incidentes, estableciendo la acción a tomarse al recibir un reposte de un evento en la seguridad de la información.
- ✓ Establecer un punto de contacto para el reporte de eventos en la seguridad de la información, dicho punto de contacto debe ser conocido por toda la empresa; además, siempre deberá estar disponible.

DOMINIO	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	16.1.3 Notificación de puntos débiles de la seguridad.		

DESARROLLO

Propósito: 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.

Recomendación: Todos los usuarios empleados, contratistas y terceros debieran reportar estos temas al Responsable de Seguridad de la Información lo más rápidamente posible para evitar incidentes en la seguridad de la información. El mecanismo de reporte debiera ser fácil, accesible y estar disponible.

Los usuarios empleados, contratistas y terceros debieran ser advertidos de no tratar de probar las debilidades de seguridad sospechadas. La prueba de las debilidades podría ser interpretada como un mal uso potencial del sistema y también podría causar daños al sistema o servicio de información y resultar en la responsabilidad legal para la persona que realiza la prueba.

Actividades:

- ✓ Dar a conocer a los empleados, contratistas y terceros el proceso de notificación de puntos débiles de seguridad.

DOMINIO	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	16.1.6 Aprendizaje de los incidentes de seguridad de la información.		
DESARROLLO			

Propósito: Definir un procedimiento que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías.

Recomendación: Se debiera utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Actividades:

Evaluar la información obtenida a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

DOMINIO	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**OBJETIVO**	Gestión de incidentes de seguridad de la información y mejoras.
CONTROL	16.1.7 Recopilación de evidencias.		
DESARROLLO			

Propósito: Recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

Recomendación: desarrollar y seguir los procedimientos internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una empresa.

En general, las reglas de evidencia debieran abarcar:

- **Admisibilidad de la evidencia:** si la evidencia se puede o no se puede utilizar en la corte.
- **Peso de la evidencia:** la calidad e integridad de la evidencia.

Actividades

- ✓ Para los documentos en papel: el original se debe mantener de manera segura con un registro de la persona quien encontró el documento, el lugar donde se encontró el documento, cuándo se encontró el documento y quién presenció el descubrimiento, cualquier investigación debe asegurarse que no se alteren o manipulen los originales.
- ✓ Para la información en medios de cómputo: se deben realizar imágenes dobles o copias de cualquier medio e información en discos duros o en memoria para asegurar su disponibilidad; manteniendo un registro de todas las acciones realizadas durante el proceso de copiado y el proceso debiera ser atestiguado; el medio original y el registro.

DOMINIO	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**OBJETIVO**	Continuidad de la seguridad de la información
CONTROL	17.1.1 Planificación de la continuidad de la seguridad de la información		

DESARROLLO

Propósito: determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

Recomendación: Se pudieran adoptar las siguientes medidas:

- Identificar y priorizar los procesos críticos de las actividades de la división de sistemas.
- Asegurar que todos los integrantes de la división de sistemas comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción

puede tener en la prestación de servicios de la empresa.

- Elaborar y documentar una estrategia de continuidad de las actividades de la empresa consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la empresa de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la empresa.
- Proponer las modificaciones a los planes de contingencia.

Actividades:
Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la división de sistemas frente a interrupciones imprevistas.

- ✓ Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la dependencia división de sistemas
- ✓ Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- ✓ Identificar los controles preventivos.
- ✓ Desarrollar un plan estratégico.

DOMINIO	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**OBJETIVO**	Continuidad de la seguridad de la información
CONTROL	17.1.2 Implantación de la continuidad de la seguridad de la información		

DESARROLLO

Propósito: establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

Recomendación:

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a

la evaluación de las dependencias de actividades externas y a los contratos vigentes.

- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.
- Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:
  - Objetivo del plan.
  - Mecanismos de coordinación y comunicación entre equipos de personal involucrado.
  - Procedimientos de divulgación.
  - Requisitos de la seguridad.
  - Procesos específicos para el personal involucrado.
  - Responsabilidades individuales.
- Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Actividades: Restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable.
La gerencia debiera asegurarse que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el local principal.

DOMINIO	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**OBJETIVO**	Continuidad de la seguridad de la información
CONTROL	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		

DESARROLLO

Propósito: verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.

Recomendación:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.

- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor

Actividades:
Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la empresa. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad de la empresa para su aprobación.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Cumplimiento de los requisitos legales y contractuales
CONTROL	18.1.1 Identificación de la legislación aplicable.		

DESARROLLO

Propósito: identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la empresa todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la empresa para cumplir con estos requisitos.

Recomendación: Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

Actividades: Definir y documentar los controles y responsabilidades individuales específicos para satisfacer estos requerimientos.
.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Cumplimiento de los requisitos legales y contractuales

CONTROL	18.1.2 Derechos de propiedad intelectual (DPI).

DESARROLLO

Propósito: implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.

Recomendación: La empresa debería considerar los siguiente lineamientos:

- Una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos de software e información.
- Sólo adquirir software a través de fuentes conocidos y acreditados para asegurar que no sean violados los derechos de autor.
- Mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual y las medidas disciplinarias aplicables a su transgresión.
- Mantener un registro de los activos e identificar todos aquellos protegidos por el derecho de propiedad intelectual.
- Mantener prueba y evidencia de la propiedad de las licencias, discos originales, manuales, etc.
- Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
- Chequear que sólo se instalen softwares autorizados y productos con licencia.
- Proporcionar una política para mantener las condiciones de licencias en forma adecuada.
- Proporcionar una política para eliminar o transferir software a terceras partes.
- Utilizar las herramientas de auditoría apropiadas.

Actividades:

.

- ✓ Adquirir el software solamente a través de fuentes conocidas.
- ✓ Mantener los documentos que acrediten la propiedad de licencias.
- ✓ Comprobar que se instale solo software autorizado y productos bajo licencia.
- ✓ Establecer una política de mantenimiento y de eliminación de software no autorizado.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Cumplimiento de los requisitos legales y contractuales
CONTROL	18.1.3 Protección de los registros de la organización		

DESARROLLO

Propósito: proteger los registros de la empresa contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Recomendación: Los registros críticos de la empresa se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la empresa.
Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

TIPO DE REGISTRO	SISTEMA DE INFORMACIÓN	PERIODO DE RETENCION	MEDIO DE ALMACENAMIENTO	RESPONSABLE

- Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.
- Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.
- El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal. Asimismo, permitir una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la empresa.

Actividades:
Realizar un inventario de información clave y los controles para la protección de los registros y la información contra pérdida, destrucción o falsificación.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Cumplimiento de los requisitos legales y contractuales

CONTROL	18.1.4 Protección de datos y privacidad de la información personal.

DESARROLLO

Propósito: garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.

Recomendación: Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

La empresa podría incluir un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los empleados y contratistas. La copia firmada del compromiso será retenida en forma segura por el por la empresa. Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer publicar información a ninguna persona, salvo autorización previa y escrita del responsable de la seguridad de la información.

Actividades: Desarrollar e implementar una política de protección y privacidad de los datos. Esta política debe ser comunicada a todas las personas involucradas en el procesamiento de información personal.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Revisiones de la seguridad de la información
CONTROL	18.2.2 Cumplimiento de las políticas y normas de seguridad.		

DESARROLLO

Propósito: revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.

Recomendación: revisar con regularidad según el área de responsabilidad el cumplimiento del procesamiento de información con las políticas de seguridad adecuadas, las normas y cualquier otro requisito de seguridad establecido.
Si se halla algún incumplimiento como resultado de la revisión, se deberían:

- Determinar la causa del incumplimiento.
- Evaluar la necesidad de acciones para garantizar que no se presenten

incumplimientos.
- Determinar e implementar la acción correctiva apropiada.
- Revisar la acción correctiva que se ejecutó.

Actividades: Detectar algún incumplimiento y determinar las causas, evaluar la necesidad de acciones correctivas, implementarlas, revisar dicha acción mediante su registro e informarlo.

DOMINIO	CUMPLIMIENTO.	**OBJETIVO**	Revisiones de la seguridad de la información
CONTROL	18.2.3 Comprobación del cumplimiento		

DESARROLLO

Propósito: revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la empresa.

Recomendación: Verificar periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

La verificación del cumplimiento debiera comprender pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados.

Actividades
- ✓ Realizar manualmente (respaldado por las herramientas de software apropiadas, si fuese necesario) el chequeo del cumplimiento técnico por un especialista experimentado y/o con la asistencia de herramientas automatizadas que generen un reporte técnico.
- ✓ Planificar, documentar y repetir las pruebas de intrusión o evaluaciones de vulnerabilidad (Ethical hacking).
- ✓ Realizar la verificación de cumplimiento técnico por personal competente y autorizado o bajo su supervisión.