PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CORPORACIÓN AUTÓNOMA REGIONAL DEL ALTO MAGDALENA – CAM

Control de Versiones	Fecha
Versión 1	30 de Enero de 2020

Carrera 1 No. 60 -79 Barrio Las Mercedes
Neiva – Huila (Colombia)
Teléfono (578) 8765017
Correo: camhuila@cam.gov.co
www.cam.gov.co

INTRODUCCIÓN

Conforme lo establece el artículo 23 de la Ley 99 de 1993, la Corporación Autónoma Regional del Alto Magdalena, es un ente corporativo de carácter público, creado por la Ley, integrado por las entidades territoriales que por sus características constituyen geográficamente un mismo ecosistema o conforman una unidad geopolítica, biogeográfica o hidrogeográfica, dotada de autonomía administrativa y financiera, patrimonio propio y personería jurídica, encargada por la ley de administrar dentro del departamento del Huila, el medio ambiente y los recursos naturales renovables y propender por su desarrollo sostenible, de conformidad con las disposiciones legales y políticas del Ministerio del Medio Ambiente.

En su estructura orgánica, dentro de la Oficina de Planeación se encuentra la oficina de Gestión Informática y Tecnológica, la cual debe encargarse de mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene la Corporación, además de seguir con los lineamientos establecidos por las demás entidades del gobierno garantizando que las acciones tendientes al funcionamiento de la entidad cumplan la normatividad vigente.

La oficina de Gestión Informática y Tecnológica apoya todas las labores misionales y corporativas de la CAM, que se encargan de garantizar la integridad y confiabilidad absoluta de todos los activos de información disponibles; El Plan de Privacidad y Seguridad de la Información es importante ante la posible pérdida, destrucción, robo y otras amenazas, y hace parte integral de la Estrategia de Gobierno Abierto.

1. OBJETIVOS

Objetivo General

Garantizar la disponibilidad, integridad y confidencialidad dela información, permitiendo preservar la privacidad de los datos de la Corporación Autónoma Regional del Alto Magdalena – CAM.

Objetivos Específicos

- Actuar conforme a la normatividad vigente a nivel Nacional las políticas de gestión y administración de activos de información de la Corporación.

- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en la Corporación.

- Establecer controles para el acceso a los activos de información de la Corporación.

- Formular el esquema de seguridad de la información de acuerdo a las necesidades y recursos de la CAM.

- Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.

2. JUSTIFICACIÓN

Para la CAM, la seguridad en la información es muy importante, y ha trabajado por garantizar la calidad, disponibilidad, veracidad y confidencialidad; teniendo en cuenta que la información ahora está expuesta a amenazas y vulnerabilidades. Para el manejo de la información existe la necesidad de su aseguramiento por medio de políticas y controles, que garanticen la estabilidad y confiabilidad de la información.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno Abierto, y el conjunto de normativas que rigen al respecto, conjuntamente con la situación actual del sistema de información y los servicios tecnológicos de la CAM, es imprescindible articular esfuerzos tendientes a ofrecer seguridad en la información, previendo las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en redes, en servicios y herramientas tecnológicas dispuestas para tal fin.

El plan de Seguridad y Privacidad De La Información comprende procesos de copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta. Que beneficia a la alta dirección y a los usuarios finales que utilizan los servicios tecnológicos de la Corporación.

3. ALCANCE

El alcance del Plan de seguridad y privacidad de la información, pretende cubrir los componentes principales del Sistema de Información Ambiental Corporativo y tecnológico de la CAM y se actualizará permanentemente de acuerdo con los requerimientos tecnológicos e informáticos que se requieran para el funcionamiento adecuado.

La implementación de este plan se realizará con el liderazgo de la oficina de Gestión Informática y tecnológica y la Oficina de Planeación, y la adopción será responsabilidad de todos los Empleados de planta, administrativos y contratistas según las competencias establecidas.

4. SEGURIDAD DE LA INFORMACIÓN

Seguridad Física

Se refiere a controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

De igual manera se pueden tener acciones que pongan en riesgo la infraestructura física que soporta los servicios tecnológicos en donde se alojan los activos de información de la CAM.

Protección de la información y de los bienes informáticos

El usuario o funcionario deberán reportar de forma inmediata a oficina de Gestión Informática y Tecnológica, cuando detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, el funcionario o contratista tiene la obligación de proteger las unidades de almacenamiento que se encuentre bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Es responsabilidad del funcionario o contratista evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo que tenga asignados.

Protección y ubicación de los equipos

Los Empleados de planta, administrativos y contratistas no deben mover o reubicar los equipos de cómputo, instalar o desinstalar software no autorizado, ni retirar sellos de los mismos, sin autorización, en caso de requerir este servicio deberá solicitarlo a la oficina de Gestión Informática y Tecnológica de la Corporación.
El equipo de cómputo asignado, deberá ser de uso exclusivo de las funciones de los Empleados de planta, administrativos y contratistas de la CAM
.
Es responsabilidad de los Empleados de planta, administrativos y contratistas almacenar su información únicamente en la partición del disco duro diferente a la destinada para archivos de programa y sistemas operativos o indicada por el personal a cargo.

El funcionario o contratista no podrá abrir o destapar los equipos de cómputo, sólo personal calificado de la oficina de Gestión Informática y Tecnológica puede realizar este trabajo, se debe evitar colocar objetos encima del equipo de cómputo u obstruir las salidas de ventilación del monitor o de la CPU, así mismo el cuidado de los equipos de impresión de la Corporación.

Mantenimiento de equipos de cómputo

Únicamente el personal autorizado podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los empleados de planta, administrativos y contratistas deberán asegurarse de respaldar en copias de seguridad la información relevante cuando el equipo sea enviado a reparación, previniendo así la pérdida involuntaria de información derivada del proceso de reparación.

El mantenimiento preventivo de los equipos de cómputo de la Corporación (computadores de escritorio, computadores portátiles, impresoras, escáner) se realizarán 2 veces al año, para los servidores, equipos de almacenamiento y dispositivos se realizarán una vez al año.

Perdida de equipo

El funcionario o contratista que tenga bajo su responsabilidad o asignado algún equipo es responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

5. SOFTWARE IDENTIFICADO EN LA CAM

Identificados bajo el estándar ISO/IEC 27000: Norma técnica con la descripción general y vocabulario sobre la administración de sistemas de seguridad de la información.

Sistema Financiero Y Contable HASNET

Es el sistema financiero y contable con el que cuenta la Corporación Autónoma regional del Alto Magdalena - CAM. Este es un sistema gráfico integrado modular, es de fácil manejo y muy flexible para ajustarse a los cambios en la normatividad del sector público, al ser un sistema Cliente - Servidor se encuentra instalado en los equipos de los usuarios finales que así lo requieren. El sistema se encuentra funcionando, utilizado para gestionar operaciones de ingresos, gastos, pagos y demás transacciones derivadas de las áreas de tesorería y contabilidad, como también del banco de proyectos, requiere una base de datos en SQLServer .

Página WEB

Portal corporativo desarrollado en Joomla, es administrado por el personal de soporte outsourcing contratista, adscritos al proyecto de gestión informática y tecnológica de la CAM.

Correo Corporativo
Se utiliza para la comunicación de los Empleados de planta, administrativos y contratistas, el correo corporativo GMAIL, es administrado desde su plataforma de por el personal de soporte outsourcing contratista, adscritos al proyecto de gestión informática y tecnológica de la CAM.

Intranet WEB

Plataforma web interna, desarrollada en Joomla, se encuentra actualizada tiene acceso desde el portal web. Instalada en un servidor local Linux, es utilizada frecuentemente para consultar la documentación del Sistema Integrado de Gestión.

Vital

Plataforma Ventanilla Integral de Trámites Ambientales en Línea VITAL, herramienta utilizada para registrar, gestionar y consultar los trámites ambientales en línea de la Corporación, para dar cumplimiento al decreto 2041 de 2014, plataforma desarrollada y administrada por la Autoridad Nacional de Licencias Ambientales ANLA. Las solicitudes se registran en la plataforma VITAL, se digitalizan y cargan los soportes documentales. Se actualiza con frecuencia debido a la rotación de personal y sin embargo se identifican trámites sin finalizar o incompletos en ocasiones.

SILA

Plataforma Sistema de Información para la Gestión de Trámites Ambientales SILA, es un Software utilizado para la Gestión de Trámites a la medida de las Autoridades Ambientales. El cual permite:
* Consulta y descarga de documentos enviados por los usuarios solicitantes.
* Expedición de Actos Administrativos.
* Expedición de Oficios de Requerimientos.
* Programación de Visitas Técnicas.

Orfeo
Es una herramienta de gestión documental de software libre amparada bajo la licencia GNU GPL, altamente escalable, desarrollada bajo PHP, que incorpora la idea de facilitar la gestión de los documentos de cualquier empresa.

Herramientas SIG (ArcGis)

ArcGIS es llamado el conjunto de productos de software en el campo de Sistemas de Información Geográfica o SIG, se reúnen diferentes aplicaciones para la edición, tratamiento, diseño, impresión y análisis de la información geográfica.

Comunicación Interna (SPARK)
Spark es un cliente de mensajería instantánea ideal para crear una red interna, la mayor diferencia que tiene con el resto de programas similares, es su interfaz es mucho más agradable, amigable y fácil de utilizar.
Tiene un cómodo sistema de envío de archivos con barra de progreso, simplemente arrastrar y soltar; salas de chat para múltiples personas. Su administración es mediante Openfire, Integrado con Active Directory, para una mejor administración y autenticación con el mismo usuario de dominio.

Aplicativo (**C.I.T.A**)
Es una herramienta (software) en la plataforma WEB llamado Centro de Información de **Tramites Ambientales** (**C.I.T.A**), para la autorización de los procedimientos de **trámites** del macroproceso Autoridad Ambiental.

Bases de Datos
Programa capaz de almacenar gran cantidad de datos, relacionados y estructurados, que pueden ser consultados rápidamente de acuerdo con las características selectivas que se deseen, motores de bases de datos Utilizados en la corporación, Oracle, SQLServer, MYSQL y MariaDB, en estos motores se manejan las diferentes bases de datos de las aplicaciones, pagina web, intranet, etc.

6. RESPALDO DE LA INFORMACIÓN

Las copias de seguridad que están disponibles en la Corporación son las siguientes:

- **Discos Duros**: Dispositivos de almacenamiento internos y externos asignados a Empleados de planta, administrativos y contratistas, se realiza en ellos los Backup realizados manualmente cada vez que crea necesario y reposará bajo su custodia, allí el usuario almacenará la información que el considere vital.

- **Carpetas Compartidas**: Se destina de un servidor, donde se crea una carpeta por cada dependencia, y carpetas a los usuarios que lo requieran, con un nombre de usuario de red y solamente este usuario tendrá todos los permisos para guardar directamente la información que considere necesaria.

- **Servidor de Almacenamiento**: Donde se guardan copias periódicas o cuando se considere necesario, es también donde se encuentran las carpetas compartidas y únicamente es administrado por el personal de Sistemas.
Para realizar un análisis de todos los elementos de riesgos a los cuales están expuestos los equipos informáticos y la información procesada por la CAM, se iniciará describiendo los activos que se pueden encontrar dentro de las tecnologías de información y la comunicación de la Corporación:

7. ACTIVOS SUSCEPTIBLES DE DAÑO

El Personal, Hardware, Software, Periféricos, Datos, información, Documentación Física y magnética, Suministro de energía eléctrica y Suministro de telecomunicaciones.

Posibles daños

- Dificultad de acceso a los recursos debido a problemas físicos en las instalaciones.
- Inconvenientes de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información.
- Divulgación de información a instancias fuera de la Corporación y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

Fuentes De Daño

- Acceso no autorizado.
- Ruptura de las claves de acceso al sistema informático.
- Desastres naturales.
- Fallas de Personal (Enfermedad, Accidentes, Renuncias, Abandono de su puesto de trabajo).

- Fallas de Hardware (Falla en los Servidores o Falla en el hardware de los dispositivos de Red.
- Falla en el servicio del proveedor de Internet.
- Fallas provocadas por manos criminales.
- Fallas Eléctricas.

8. IDENTIFICACIÓN DEL RIESGO

Riesgo: Perdida de información, perdida de la confidencialidad e integridad de la información por faltas en la seguridad informática en beneficio de un particular.
Causas:

- Generación de información confusa o errada sobre los temas de la entidad.
- Falta de unidad de criterio sobre el manejo de los temas
- Incumplimiento en la entrega de los productos finales.
- Falta de capacitación para implementar actualizaciones normativas y procedimentales
- Cambio de la normatividad relacionada con TIC que impliquen modificación de las actividades.
- Falencias en la generación de copias de seguridad de los equipos servidores.
- Falencias en los controles de seguridad informática.
- Fallas y errores en la infraestructura tecnológica.

Minimización Del Riesgo
Corresponde al presente Plan de Seguridad Informática de la CAM minimizar estos índices con medidas preventivas y correctivas sobre los riesgos más relevantes.

- **Falla En Los Equipos**

La falla en los equipos pocas veces se debe a falta de mantenimiento y limpieza. El daño de equipos se puede presentar, por fallas en la energía eléctrica, algunos equipos no cuentan con dispositivos que amplíen el tiempo para apagar el equipo correctamente, equivocaciones de forma involuntaria con respecto al manejo de información, software y equipos.
Se presentan dudas e inquietudes en el manejo de los equipos de cómputo por parte de Empleados de planta, administrativos y contratistas.

Acción Preventiva
Realizar mantenimiento preventivo de equipos de cómputo e impresoras anualmente, según cronograma.
El administrador de la red debe asignar permisos y privilegios a cada usuario de acuerdo a sus funciones y/o competencias.
Capacitar en temas de informática básica y asistencia como soporte para la realización de las actividades.

- **Acción De Virus Informático**
La Corporación cuenta con software antivirus ESET, Sólo la oficina de Gestión Informática y tecnológica es la encargada de realizar la instalación del software antivirus en cada uno de los equipos.

Acción Preventiva
Mantener actualizadas las licencias, descargar las actualizaciones más recientes de la base de datos, crear tareas y políticas para la protección de los equipos cliente y servidores.

- **Accesos No Autorizados**
Se controla el acceso al sistema de red mediante un administrador con su respectiva clave, la asignación de los usuarios se realiza en Gestión Informática y Tecnológica. Se inactivan los usuarios del personal que se retira de la Corporación tan pronto como se tenga el aviso por parte de la administración de talento humano.
Las contraseñas de inicio de sesión a las aplicaciones y programas de la CAM son exclusivas de Empleados de planta, administrativos y contratistas, dichas contraseñas se mantienen vigentes en tanto el personal esté vinculado a la Corporación.

- **Firewall Fortinet 100E**
Brinda la posibilidad de gestionar el acceso aplicaciones, sitios web de la Corporación, creando reglas de seguridad y restringiendo la exposición de la red hacia el exterior. Conexiones VPN para cuando los funcionarios requieran acceso a la red desde sitios externos.

8. RECUPERACIÓN Y RESPALDO DE LA INFORMACIÓN

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Corporación, Se establece los procedimientos relativos a: Sistemas e Información, Equipos de Cómputo, Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

a) Sistemas de Información
La Corporación cuenta con una relación de los Sistemas de Información de software de datos, para respaldarla con backups.

b) Equipos de Cómputo
Se debe tener en cuenta el inventario de Hardware, impresoras, scanner criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.
- Señalización o etiquetamiento de las computadoras de acuerdo a la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación o buscar información importante, en este caso aplica los servidores de aplicaciones y carpetas compartidas.
- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la corporación.

9. GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO (BACKUPS)

En el procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

- Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores.
- Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.
- Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de respaldo, debidamente marcadas, estas se harán en un sistema de almacenamiento.
- Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.
- Se utilizará el programa WINRAR u otra aplicación GNU-GLP o de prueba para comprimir el listado de archivos o carpetas a respaldar.

10. RECOMENDACIONES PARA EQUIPOS DE CÓMPUTO

Poner especial atención a las actualizaciones del navegador web, el sistema operativo como Windows es propenso a fallos, riesgo que puede ser aprovechado por delincuentes informáticos, frecuentemente se liberan actualizaciones que solucionan dichos fallos.

- Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, nos 'ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el proceso de Gestión de TIC en antivirus, GMAIL, office, navegadores y otros programas.
- Tener el antivirus actualizado con frecuencia. Escanear con el antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados por internet.
- Estar pendiente de la fecha de caducidad de la licencia con el fin de renovarla inmediatamente tan pronto esta se cumpla.
- Es recomendable tener instalado en los equipos algún tipo de software antispyware para evitar que se introduzcan en el equipo programas espías destinados a recopilar información confidencial sobre el usuario.
- Para prevenir infecciones por virus informático, los usuarios de la CAM no deben hacer uso de software que no haya sido proporcionado y validado por La Gestión Informática y Tecnológica.
- Los Empleados de planta, administrativos y contratistas con asesoría de los profesionales de la oficina de Gestión Informática y Tecnológica, deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado antes de ejecutarse.
- Ningún funcionario, contratista o personal externo, podrá descargar software, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la oficina de Gestión Informática y Tecnológica.

11. NAVEGACIÓN EN INTERNET Y LA UTILIZACIÓN DE CORREO ELECTRÓNICO

Navegue por páginas web seguras y de confianza, para identificarlas verifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad, extreme la precaución si va a facilitar información confidencial a través de internet.
Utilizar contraseñas seguras, es decir aquellas compuestas por ocho caracteres, como mínimo y que combinen letras, números y símbolos.
Tratamiento de su correo electrónico, ya que este se ha convertido en una de las formas más utilizadas para introducir código malicioso, llevar a cabo estafas, introducir virus, etc.

12. USO DE DISPOSITIVOS EXTRAÍBLES

El Funcionario o usuario que tenga asignados estos tipos de dispositivos será responsable del buen uso de ellos.

- La persona encargada de administrar cada equipo deberá velar por el uso adecuado de dispositivos de almacenamiento externo, como Pen drives, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- Cada vez que se inserte un dispositivo externo a la red de la corporación, deberá ser analizado con el software del antivirus.

13. GLOSARIO

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6) Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).