EPSA CETSA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OSCAR IVAN ZULUAGA SERNA
GERENTE GENERAL

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. LÍNEA BASE DE LA POLÍTICA 3
3.1 RESPONSABILIDAD 3
3.2 CUMPLIMIENTO 3
3.3 EXCEPCIONES 3
3.4 ADMINISTRACIÓN DE LAS POLÍTICAS 3
4. DESCRIPCIÓN LAS POLÍTICAS Y ESTÁNDARES 4
4.1 ORGANIZACIÓN DE SEGURIDAD 4
4.2 CLASIFICACIÓN Y CONTROL DE ACTIVOS 5
4.3 USO ACEPTABLE DE LOS ACTIVOS Y RECURSOS 6
4.4 TRATAMIENTO Y GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN 12
4.5 SEGURIDAD DEL PERSONAL 13
4.6 SEGURIDAD FÍSICA Y DEL ENTORNO 14
4.7 CONTROL DE ACCESO 15
4.8 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 17
4.9 GESTIÓN DE SEGURIDAD PARA TELECOMUNICACIONES E INFRAESTRUCTURA DE TIC 18
4.10 GESTIÓN DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 21
4.11 CUMPLIMIENTO Y NORMATIVIDAD LEGAL 22
5. DOCUMENTACIÓN RELACIONADA 24
6. DEFINICIONES 24

1. OBJETIVO

Establecer las medidas organizacionales, técnicas, físicas y legales, necesarias para proteger los activos de información contra acceso no autorizado, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental.

2. ALCANCE

Esta Política es aplicable a todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de la organización.

3. LÍNEA BASE DE LA POLÍTICA

3.1 Responsabilidad

Es responsabilidad de la Gerencia de Gestión de Tecnología hacer uso de la Política de Seguridad de la Información, como parte de sus herramientas de gobierno y de gestión, de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

3.2 Cumplimiento

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los colaboradores, consultores, contratistas, terceras partes violan estas políticas, la organización se reserva el derecho de tomar las medidas correspondientes.

3.3 Excepciones

Las excepciones a cualquier cumplimiento de Política de Seguridad de la Información deben ser aprobadas por la Gerencia de Gestión de Tecnología, la cual puede requerir autorización de la Gerencia General EPSA, la Vicepresidencia de Desarrollo Corporativo y Nuevos Negocios, del Comité de Asuntos Corporativos o de la Presidencia de la compañía. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas.

3.4 Administración de las políticas

Las modificaciones o adiciones de la Política de Seguridad de la Información serán propuestas por la Gerencia General de EPSA, Vicepresidencia de Desarrollo Corporativo y Nuevos Negocios de Celsia, por medio de las áreas de Arquitectura Organizacional de Celsia y/o de

Gestión de Tecnología de EPSA y serán aprobadas por el Comité de Asuntos Corporativos de Celsia. Estas políticas deben ser revisadas como mínimo una vez al año o cuando sea necesario.

4. DESCRIPCIÓN DE LAS POLÍTICAS Y ESTÁNDARES

Generalidades

La información es un activo que la compañía considera esencial para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

A través de esta Política se difunden los objetivos de seguridad de la información de la compañía, que se consiguen a través de la aplicación de controles de seguridad, para gestionar un nivel de riesgo aceptable. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos de negocio y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en EPSA.

Los principios de la política son parte de la cultura de la empresa, por lo que se asegura un compromiso por parte del Comité de Gerencia de EPSA para la difusión, consolidación y cumplimiento de la presente política.

4.1 Organización de seguridad

Política de la organización de seguridad

La Gerencia de Gestión de Tecnología a través del oficial de seguridad de la información es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en EPSA y reportará al Comité de Seguridad de la Información, dicho comité debe contar con la presencia de personal clave y claramente definido, con el objeto de cumplir y soportar las actividades de Seguridad de la Información.

Estándares de la Política de la organización de seguridad

- **Responsabilidades para la seguridad de la Información**.
  EPSA es el propietario de la información. Su tenencia y manejo es delegada a los Gerentes, quienes son responsables de la custodia de la información que las gerencias generan, considerando su propósito y uso. Por ello los Gerentes deben ser conscientes de

los riesgos a la que está expuesta la información a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para disminuirlos.

- **Contacto con autoridades y grupos de interés.**
  EPSA debe mantener contacto con las autoridades y grupos especiales de interés para estar al corriente en cambios de normativa del gobierno electrónico en Colombia e identificar las tendencias en Seguridad de la Información.

- **Revisión independiente en seguridad de la información**.
  Auditoría Interna debe implementar y ejecutar un plan interno de auditoría de seguridad de la información. Este plan debe estar enfocado hacia la revisión de todos los requerimientos (políticas y procedimientos) de seguridad. Los resultados deben generar un programa de seguridad, que incluya como mínimo: acciones a realizar, tablas de tiempo y responsables. El programa debe ser aprobado por el Comité de Seguridad de la Información.

- **Seguridad en los Accesos por Terceros**.
  El Oficial de Seguridad de la Información debe realizar una evaluación de riesgos para identificar el riesgo de acceso por terceros a la información de EPSA. Cada gerencia debe verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

4.2 Clasificación y control de activos de Información

Política para la clasificación y control de activos de información

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada como secreta, restringida o general.

La información secreta y restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

Estándares de la Política de clasificación y control de activos de información

- **Responsabilidad sobre los activos**.
  EPSA pone al servicio de los colaboradores el uso de los medios necesarios para el normal desarrollo de las labores propias de sus respectivos cargos, para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta.

- **Metodología de clasificación de activos.**
  Para asegurar que los activos de información reciben el nivel de protección adecuado, la Gerencia de Gestión de Tecnología es responsable de definir la metodología de clasificación de activos de información, estos se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.

4.3 Uso aceptable de los activos y recursos

Política de Uso Aceptable de los Activos y Recursos de información

Todos los colaboradores, consultores, contratistas, terceras partes, que usen activos de información que sean propiedad de EPSA, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados.

Estándares para el uso aceptable de los activos de información

- **Uso de los sistemas y equipos de cómputo**.
  La organización tiene regla de renuncia (disclaimer) que debe utilizarse al inicio de sesión en los equipos de cómputo:

  "Advertencia! Este sistema (hardware, software y periféricos), así como la información en él contenida es propiedad de la empresa y su uso está restringido únicamente para propósitos de su negocio, reservándose el derecho de monitorearlo en cualquier momento. Cualquier utilización, modificación o acceso no autorizado a este sistema dará lugar a las acciones disciplinarias y/o legales que correspondan. El ingreso y utilización de este sistema implica su consentimiento con esta política."

- **Correo electrónico.**
  La organización, como muestra del respeto por los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o que reciba por medio del sistema de correo electrónico propiedad de la compañía; en consecuencia, podrá denegar el acceso a los servicios de correo electrónico, inspeccionar, monitorear y/o cancelar un buzón de correo asignado.

  Las comunicaciones por correo electrónico entre la empresa y sus públicos de interés deben hacerse a través del correo homologado y proporcionado por la empresa. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés de la organización, ni para transmitir cualquier otro tipo de información del negocio.

A los colaboradores que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna en el servidor una vez son vinculados. La Gerencia de Gestión Humana es responsable de informar a la Gerencia de Gestión de Tecnología, las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de colaboradores para la suspensión de este servicio.

Esta cuenta estará activa durante el tiempo que dure la vinculación del colaborador con la compañía, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de servicios.

La capacidad máxima para almacenamiento de correo electrónico está definida por la Gerencia de Gestión de Tecnología y depende del tipo de usuario. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad. De igual manera, en caso de necesidad (por razones del negocio o técnicas), las capacidades máximas de los buzones podrán ser modificadas unilateralmente por parte de la compañía.

El sistema de monitoreo filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.

La organización tiene regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes. Para evitar reclamaciones legales todos los usuarios de correo de la empresa tienen que hacer pública la renuncia de responsabilidad legal por el envío de la información. El disclaimer aprobado es:

La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente y bórrela puesto que su uso no autorizado acarreará las sanciones y medidas legales a que haya lugar. La empresa no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información.

"The information contained in this message and its attachments is strictly confidential. If you received this communication in error, please immediately notify the sender of the situation by replying it to sender email address and delete this message as its unauthorized use shall derive in applicable penalties and legal actions.. The Company is not liable for the presence of any virus or malware in this message or its attachments that cause or may cause damage to your equipment, software or that affects your information."

El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptar el buzón otorgado por la organización, el usuario se compromete a:

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
- El colaborador titular de correo o cuenta asignada por la organización, usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo o de las investigaciones que tenga asignadas; las únicas Gerencias autorizadas para el envío de correos masivos son Gestión Humana, Comunicaciones, Gestión de Tecnología, Seguridad Física, Compras Logística y Servicios. Otras necesidades de comunicación masiva deben ser aprobadas por las Gerencias de Gestión de Tecnología y Comunicaciones.
- El uso del correo electrónico propiedad de la compañía debe ser usado solamente para fines propios a la organización. En su uso el colaborador actuará siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofendan la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.
- No podrá recibir o enviar mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificar plenamente su autor; adicionalmente, los colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.
- Los colaboradores de la compañía se abstendrán de utilizar la cuenta para el envío o reenvío de mensajes *spam* (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), *hoax* (es un intento de hacer creer que algo falso es real), con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.
- Evitar el envío desde su buzón de elementos (textos, *software*, música, imágenes o cualquier otro) que contravengan lo dispuesto en la legislación vigente y en los reglamentos internos, sobre propiedad intelectual y derechos de autor. En especial, es necesario evitar la distribución de *software* que requiera licencia, claves ilegales de *software*, programas para romper licencias (*crackers*), y en general, cualquier elemento u objeto de datos sin permiso específico del autor cuando este sea requerido. La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario, con perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
- Realizar mantenimiento periódico de su correo, cuando el sistema le haga advertencias de espacio disponible. Estas advertencias se realizan varias veces, por lo que debe estar atento e informar a la mesa de servicios informáticos, cuando requiera la depuración del mismo.
- Utilizar la cuenta de correo electrónico corporativa para fines laborales, de investigación y los estrictamente relacionados con las actividades propias de su

trabajo. Los colaboradores deben evitar usar el buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés de la empresa.

- El colaborador debe depurar mensualmente el contenido del buzón de entrada en el servidor para evitar que los mensajes permanezcan en él un tiempo excesivo que conduzca a la congestión o al bloqueo del mismo.
- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa.
- Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.
- Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. Podría tratarse de un virus. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando.
- En lo posible, es necesario evitar usar letras mayúsculas, especialmente en el campo de “Asunto:”, al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, ¡, !, ¿), esto puede hacer que los sistemas de correo lo identifiquen como correo no deseado o *spam*, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.
- Si utiliza el servicio de correo a través del sitio web de la empresa, se recomienda que no deje mensajes almacenados por mucho tiempo en el servidor de correo. Tenga presente descargarlos con frecuencia, preferiblemente a diario. Tenga en cuenta que el tamaño de su buzón de correo es limitado; una vez superado este tope, el sistema no le procesará más correos. Elimine mensajes si lo necesita y vacíe la papelera siempre que sea posible.

- **Navegación en Internet**.
  El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la organización y deben ser utilizados por el colaborador para realizar las funciones establecidas para su cargo, por lo cual la compañía definió los siguientes parámetros para su uso:

  - El colaborador debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía *web* o medios magnéticos.
  - La descarga de música y videos no es una práctica permitida.
  - Evitar el uso de servicios descarga de archivos como: *KaZaA, Emule, LimeWire, Morpheus, GNUtella* o similares.
  - Las salas de video-conferencia de la organización deben ser de uso exclusivo para asuntos relacionados con la empresa. Cualquier excepción a esta política debe ser autorizada por la Gerencia de Gestión de Tecnología.
  - Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet (*proxy*).

- El uso con fines comerciales, políticos, particulares o cualquier otro que no sea el laboral y que dio origen a la habilitación del servicio, no está permitido.
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los colaboradores de la organización; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- Los colaboradores no deberán coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que pueda infringir o violar cualquier patente, derechos de autor, marcas, secretos empresariales o cualquier otro derecho intelectual de otra persona.
- Abstenerse de coleccionar, almacenar, divulgar, transmitir o solicitar cualquier material, información, mensaje o comunicación que viole la ley o de la cual puedan surgir responsabilidades u obligaciones de carácter criminal o civil bajo cualquier ley estatal, local, nacional o internacional; incluyendo, pero no limitado, las leyes y regulaciones de control y exportación de Colombia y de los decretos sobre fraudes de computación.
- Coleccionar, almacenar, divulgar, transmitir o solicitar información personal (incluyendo sin limitación alguna, información biográfica, habitacional, social, marital, ocupacional, financiera, y de salud) sobre otros usuarios, sin su consentimiento o conocimiento, son prácticas no permitidas por la compañía.
- Los colaboradores se deben abstener de coleccionar, divulgar, transmitir o solicitar programas de computación dañinos, virus, códigos, expedientes o programas.
- Hacer ofertas fraudulentas de compra o venta, así como también, conducir cualquier tipo de fraude financiero, tales como "cartas en cadena" o "las pirámides", son faltas se constituyen como violaciones a esta Política.
- No está permitido personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal.
- Hacer o intentar hacer, cualquier cosa que afecte desfavorablemente la habilidad de utilizar el servicio de internet por otros usuarios, incluyendo sin limitación alguna, "negación de servicios", ataques contra otros sistemas o contra el anfitrión de redes u otros usuarios, se constituye como una violación a esta Política.

- **Uso de herramientas que comprometen la seguridad**.
  Hacer o intentar hacer, sin permiso del dueño o del anfitrión del sistema o de la Gerencia de Gestión de Tecnología, cualquiera de los siguientes actos:
  - Acceder el sistema o red.
  - Monitorear datos o tráfico.
  - Sondear, copiar, probar *firewalls* o herramientas de *hacking*.
  - Atentar contra la vulnerabilidad del sistema o redes.
  - Violar las medidas de seguridad o las rutinas de autenticación del sistema o de la red.

- **Recursos compartidos**.
  El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto su uso y aplicación debe ser controlado. Con este propósito la organización define los siguientes lineamientos para su uso seguro:

  - Se debe evitar el uso de carpetas compartidas en equipos de escritorio.
  - Los administradores de la red establecen e implementan, en los casos aprobados, la configuración de acceso a la carpeta, previo requerimiento formal de la misma a través de la Mesa de Servicios.
  - El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.
  - Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).
  - Debe tenerse claramente especificado el límite de tiempo durante el cual estará publicada la información y compartido el recurso en el equipo.
  - Si se trata de información confidencial o crítica para la empresa, deben utilizarse las carpetas destinadas para tal fin en el servidor de archivos de usuarios, para que sean incluidos en las copias diarias de respaldo de información o implementar herramientas para el respaldo continuo de información sobre dichos equipos.
  - El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.
  - No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus corporativo actualizado.

- **Sitios Web para compartir documentos**.
  El dueño del sitio será el responsable de la seguridad del mismo y del acceso a la información que se encuentra alojada.
  - El dueño del sitio será el responsable de otorgar los permisos requeridos.
  - El dueño del sitio definirá un delegado que tengan control total sobre el sitio, a manera de contingencia, para la asignación de los permisos requeridos en su ausencia.

- **Computación en nube**.
  Ninguna información de EPSA podrá utilizar tecnologías de computación en nube si no está previamente autorizado por la Gerencia de Gestión de Tecnología.

- **Uso equipos portátiles y dispositivos móviles.**
  Los colaboradores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la empresa, tales como escritorios y aplicaciones virtuales, correo,

comunicaciones unificadas, redes virtuales privadas (VPN), entre otros, atendiendo las siguientes directrices:

- En sitios públicos, adopte precauciones con los dispositivos móviles que no esté usando, asegurándose que se encuentre en el bolsillo, maletín o lugar no visible.
- El dispositivo móvil debe estar configurado para bloqueo automático por un tiempo de inactividad a través de medios disponibles de configuración tales como contraseña, patrón huella dactilar, reconocimiento de voz, guaya, pregunta entre otras.
- Uso de aplicación de antivirus.
- Uso de canales seguros y cifrados cuando se conecte a redes compartidas de acceso libre, no seguras.

- **Acceso de equipos distintos a los asignados.**
  - Desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.
  - No dejar claves en ningún sistema de almacenamiento de información web.
  - Creación de contraseñas seguras, no incluir información personal como nombres, fechas de nacimiento, otros.
  - Cerrado de sesión de escritorio virtual cuando no esté en uso.

La Gerencia de Gestión de Tecnología debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se compromete la información del negocio, teniendo en cuenta los riesgos que conlleva el trabajar con el equipo móvil en entornos desprotegidos.

La utilización de los servicios móviles conectados a las redes, debe tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil solo debe tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

4.4 Tratamiento y gestión del riesgo en seguridad de la información

Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

La Gerencia de Gestión de Tecnología a través del oficial de seguridad de la información, es responsable de analizar los riesgos en seguridad de la información, con base en los objetivos de negocio y de acuerdo con la Política de Gestión de Riesgos y con aprobación del Comité de Seguridad de la Información.

Las Gerencias son responsables de priorizar y realizar el tratamiento de los riesgos en seguridad de la información de acuerdo con el apetito de riesgo de la empresa.

Estándares de la Política del Tratamiento y Gestión del Riesgo en Seguridad de la Información

Periódicamente se debe realizar una valoración del riesgo para contemplar los cambios en los requisitos de seguridad y la situación de riesgo, tales como cambio en los activos, las amenazas, las vulnerabilidades y los impactos. Se debe decidir cuándo un riesgo es aceptable, ya sea por motivos de objetivos de negocio o por costes no rentables.

Los posibles tratamientos a los riesgos identificados incluyen:

- Evitar el riesgo.
- Disminuir la probabilidad de ocurrencia.
- Disminuir el impacto.
- Transferir los riesgos.
- Retener los riesgos.

4.5 Seguridad del personal

Política de Responsabilidad del Personal

La Gerencia de Gestión Humana debe notificar a la Gerencia de Gestión de Tecnología todas las novedades del personal directo e indirecto tales como ingresos, traslados, retiros y vacaciones.

Estándares de la Política de Seguridad del Personal

- **Seguridad previa a la contratación del personal**.
  Para toda persona que ingrese a la compañía, la Gerencia de Gestión Humana debe asegurar las responsabilidades sobre seguridad de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación.

- **Seguridad durante el contrato**.
  La Gerencia de Gestión Humana debe desarrollar un programa efectivo y continuo de concientización de protección de la información para todo el personal. También se requiere de capacitación específica en administración de riesgos tecnológicos para aquellos

individuos que están a cargo de responsabilidades especiales de protección y los conceptos básicos con que debe cumplir todo colaborador.

Es responsabilidad y deber de cada colaborador de EPSA asistir a los cursos de concientización en seguridad de la información que la empresa programe y aplicar la seguridad según las políticas y los procedimientos establecidos por la empresa.

- **Finalización o cambio de puesto**.
  La Gerencia de Gestión Humana debe asegurar que todos los colaboradores que salgan de la empresa o cambien de puesto de trabajo, hayan firmado un acuerdo de confidencialidad, cuyo cumplimiento será vigente hasta que EPSA lo considere conveniente, incluso después de la finalización del puesto de trabajo o del contrato.

  La Gerencia de Gestión Humana se asegurará que la salida o movilidad de los colaboradores sea gestionada hasta la completa devolución de todos los activos y retirada de los derechos de acceso.

4.6 Seguridad física y del entorno

Política de Seguridad Física y del Entorno

El centro de procesamiento de datos y cuarto de equipos de TIC, deben de estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia y deben cumplir con las políticas de seguridad física.

Estándares de la Política de Seguridad Física y del Entorno

- **Controles de acceso físico.**
  El acceso a áreas TIC restringidas sólo se debe permitir para:
  - Desarrollo de operaciones tecnológicas.
  - Tareas de aseo (monitoreado por personal de Gerencia de Gestión Tecnología).
  - Pruebas de equipos.
  - Almacenamiento de equipos.
  - Implementación o mantenimiento de los controles ambientales.

- **Escritorio limpio**.
  La implementación de una directriz de escritorio limpio permitirá reducir el riesgo de acceso no autorizado o daño a medios y documentos.

Los computadores deben bloquearse después de diez (10) minutos de inactividad, el usuario tendrá que autenticarse antes de reanudar su actividad. Todos los colaboradores, consultores, contratistas, terceras partes, deben bloquear la sesión al alejarse de su computador.

- **Seguridad de los equipos.**
  Para prevenir la pérdida de información daño, robo o el compromiso de los activos de información y la interrupción de las actividades de EPSA, los equipos deben estar conectados a la toma regulada destinada para tal fin y debidamente asegurados mediante el uso guayas para los equipos portátiles.

- **Retiro de equipos.**
  Se deben tener en cuenta los procesos de instalación y retirada del equipo, de tal manera que estos se hagan de forma controlada y segura. La protección de los equipos, incluso cuando se utilizan fuera de la oficina, es necesaria para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo.

4.7 Control de acceso a la información

Política de Control de Acceso a la Información

La Gerencia de Gestión de Tecnología, conforme la clasificación de activos de información, debe implementar las medidas de seguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida, fuga, consulta, uso o acceso no autorizado o fraudulento.

El control de acceso de datos e información sensible se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.

Estándares de Política de Control de Acceso a la Información

- **Gestión de acceso a usuarios.**
  La Gerencia de Gestión de Tecnología establecerá procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por la Gerencia responsable del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación del registro a quienes no necesiten el acceso. Se debe brindar atención y seguimiento especial, donde sea apropiado, a la necesidad del control de asignaciones de accesos privilegiados.

- **Registro de usuarios.**

Todos los usuarios deben tener una identificación única personal o jurídica, que se utilizará para el seguimiento de las actividades de responsabilidad individual o jurídica. Las actividades habituales de usuario no deben ser desempeñadas a través de cuentas privilegiadas.

En circunstancias excepcionales, por beneficio de la compañía, se podrá usar un identificador compartido, para un grupo de usuarios con trabajo específico; este debe ser autorizado y debidamente aprobado por la respectiva gerencia, previo visto bueno de la Gerencia de Gestión de Tecnología.

El usuario debe tener autorización de la respectiva gerencia para el uso del sistema o servicio de información. Se debe verificar que el nivel de acceso otorgado sea adecuado para los propósitos de la empresa y conserven una adecuada segregación de funciones. Adicionalmente, deben tomar y certificar la formación y así garantizar el uso adecuado del sistema o servicio de información.

- **Responsabilidades del usuario.**
  Una seguridad efectiva requiere la cooperación de los usuarios autorizados, quienes deben saber sus responsabilidades para el mantenimiento de controles efectivos al acceso, en particular, aquellos con referencia al uso de contraseñas, La Gerencia de Gestión de Tecnología implementará los procedimientos necesarios que permitan controlar la creación, modificación, desactivación y eliminación de usuarios, administración de contraseñas y permisos de acceso a los recursos tecnológicos y a la información. Adicionalmente, es necesario implementar un procedimiento de revisión periódica de los permisos de acceso de los usuarios.

  Los colaboradores, contratistas y terceros entienden las condiciones de acceso y deben mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de este. Esta declaración puede ser incluida en los términos y condiciones laborales. Igualmente deben cumplir las buenas prácticas en la selección y uso de la contraseña.

  - **Control de acceso a la red.**
    Únicamente se debe proporcionar a los colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos. Se deben implantar controles adicionales para el acceso por redes inalámbricas. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

  - **Control de acceso a las aplicaciones.**
    El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.

Las sesiones inactivas deben cerrarse después de un período de inactividad definido y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.

Las cuentas de usuario de herramientas o productos que vengan por omisión se deben deshabilitar inmediatamente después de la instalación de los sistemas o software.

Las contraseñas predeterminadas por el proveedor se deben cambiar inmediatamente después de la instalación de los sistemas o *software*.

La Gerencia de Gestión de Tecnología debe integrar las aplicaciones con el Directorio Activo.

4.8 Gestión de incidentes de seguridad de la información

Política de Gestión de incidentes de Seguridad de la Información

Todos los colaboradores, consultores, contratistas, terceras partes, deben anotar y comunicar cualquier punto débil que hayan observado o que sospechen que exista en los sistemas o servicios a través de la mesa de servicios.

Estándares de la Política de Gestión de Incidentes de Seguridad de la Información

- **Notificación de eventos y debilidades de seguridad de la información.**
  La Gerencia de Gestión de Tecnología debe asegurarse de que los eventos y los puntos débiles de seguridad de la información asociados con los sistemas de información, se comunican de forma que sea posible emprender acciones correctivas.

  Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, que determine la respuesta que debe darse cuando se recibe un informe de un evento de seguridad de la información.

- **Gestión de incidentes de seguridad de la información.**
  Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, el grupo de resolución de problemas se encargará de analizar la causa y evaluar conforme al proceso de gestión de problemas.

Cuando se detecta por primera vez un evento de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro que se destruyan de forma intencional o accidental de las pruebas necesarias antes de tomar conciencia de la gravedad del incidente. Se debe hacer uso de los servicios jurídicos de EPSA y/o de la Policía en las primeras fases de cualquier acción legal que se esté considerando, así como asesorarse de las pruebas necesarias.

Cuando una acción contra una persona u organización, después de un incidente de seguridad de la información, implique medidas legales (tanto civiles como penales), deberían recopilarse pruebas, que deberían conservarse y presentarse de manera que se ajusten a las normas legales vigentes.

A la hora de la recopilación de las pruebas, se preservará la cadena de custodia y se utilizarán herramientas y procedimientos aceptados de análisis forenses.

4.9 Gestión de seguridad para telecomunicaciones e infraestructura de TIC

Política de Gestión de Telecomunicaciones e Infraestructura de TIC

La Gerencia de Gestión de Tecnología debe proveer el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación, a través de una Gestión de Telecomunicaciones e Infraestructura de TIC efectiva y eficiente.

Estándares de la Política de la Política de Gestión de Telecomunicaciones e Infraestructura de TIC

- **Procedimientos y responsabilidades de operación.**
  La Gerencia de Gestión de Tecnología debe definir y documentar claramente las responsabilidades para el manejo y operación de instalaciones de computadores y redes, apoyadas por instrucciones operacionales apropiadas incluyendo procedimientos de respuesta en caso de incidentes.

  La Gerencia de Gestión de Tecnología debe definir controles que garanticen la apropiada operación tecnológica. Estos controles deben incluir como mínimo los siguientes procedimientos:
  - Copias de seguridad.
  - Verificación de cintas.

- Recuperación de datos y reversión de cambios.
- Administración de sistemas de antivirus.
- Administración de usuarios y contraseñas.
- Administración de acceso a los recursos.
- Administración de acceso remoto.
- Medición de desempeño.
- Capacidad y disponibilidad de los recursos de TI.
- Gestión de pistas de auditoria y sistemas de registro de información.
- Aseguramiento de plataformas.

- **Gestión del Cambio.**
  La Gerencia de Gestión de Tecnología debe implementar los controles necesarios que permitan garantizar la segregación de funciones y un adecuado seguimiento a los cambios efectuados a los activos críticos de TI. La documentación debe incluir, entre otros:
  - Persona que solicita el cambio.
  - Responsable de autorización.
  - Descripción del cambio.
  - Justificación del cambio para el negocio.
  - Lista de chequeo para evaluación de riesgos, sistemas y/o dispositivos comprometidos.
  - Nivel de impacto.
  - Pruebas, aprobación revisiones de post-implementación.
  - Capacitación, cuando sea necesario.

- **Segregación de funciones.**
  Las tareas y responsabilidades propias de gestión de Tecnología, se deben segregar para reducir e impedir las oportunidades de acceso no autorizado a la red y cualquier modificación o mal uso de los activos de los sistemas de información. Se prestará especial cuidado que una persona no pueda por si misma acceder, modificar o utilizar los activos, sin previa autorización.

- **Separación de Ambientes.**
  Cuando aplique los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados, prevenir fallos e implementar controles.

- **Planificación y Aceptación.**
  Se deben definir los requisitos de capacidad futura, con el fin de reducir el riesgo a una sobrecarga del sistema. Los requisitos operativos de sistemas nuevos se deben establecer, documentar y probar antes de su aceptación. Los requisitos de restitución para los servicios apoyados por diferentes aplicaciones se deben coordinar y revisar frecuentemente. Los administradores de TI deben estar alerta a los riesgos asociados a estas tecnologías, así mismo considerar la toma de medidas especiales para su prevención o detección.

- **Protección contra el código malicioso.**
  La Gerencia de Gestión de Tecnología debe implementar controles de detección, prevención y recuperación para la protección frente al código malicioso. Los usuarios deben ser conscientes de los peligros de los códigos maliciosos. En EPSA no está permitido el uso de *software* no licenciado y su instalación en cualquiera de los equipos de la compañía.

- **Copias de seguridad.**
  Se deben hacer copias de respaldo de la información y del *software*. Para garantizar la integridad y disponibilidad, se debe hacer su comprobación regular de los mecanismos y la información en conformidad con la política de respaldo acordada, conservando los niveles de confidencialidad requeridos. La Gerencia de Gestión de Tecnología debe almacenar las copias de seguridad por fuera de las instalaciones de EPSA con el fin de garantizar su recuperación en caso de un evento mayor en la sede principal.

- **Gestión de seguridad en las redes.**
  Se le debe dar atención especial al manejo de la seguridad en redes, la cual puede extenderse más allá de los límites físicos de EPSA. Procedimientos y medidas especiales se requieren para proteger el paso de información sensible a redes de dominio público. La Gerencia de Gestión de Tecnología debe garantizar que los proveedores de servicios de red implementan medidas en cumplimiento con las características de seguridad, acuerdos de niveles de servicio y requisitos de gestión.

  Se deben establecer controles especiales para salvaguardar la integridad y confidencialidad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y aplicaciones conectadas, igualmente se debe garantizar la disponibilidad de los servicios de red y computadores conectados.

- **Servicios de Comercio Electrónico.**
  Se debe realizar una evaluación para identificar el riesgo asociado con el uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles. Se debe considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

- **Monitoreo de uso del sistema.**
  El nivel de monitoreo necesario para los servicios se determinará mediante una evaluación de riesgos. EPSA cumplirá los requisitos legales que se apliquen en sus actividades de monitoreo. Se deben registrar las actividades tanto del operador como del administrador del sistema. Las actividades a monitorear incluyen: operaciones privilegiadas, acceso no autorizado y alertas o fallas del sistema, entre otras.

- **Registros de Auditoría.**
  Se deben elaborar y mantener durante un período acordado, los registros de auditoría de las actividades de usuario, de operación y administración del sistema.

- **Protección de la información de registro.**
  Los servicios y la información de la actividad de registro se deben proteger contra el acceso o manipulación no autorizados.

- **Tratamiento de medios con información.**
  Se deben controlar los medios y proteger para prevenir la revelación, modificación, eliminación o destrucción no autorizada de los activos y la interrupción de las actividades del negocio.

  La Gerencia de Gestión de Tecnología debe implementar los controles que permitan garantizar que la eliminación de cualquier dispositivo o componente tecnológico que contenga información sensible, sean destruidos físicamente, o bien que la información sea destruida, borrada o sobrescrita, mediante técnicas que no hagan posible la recuperación de la información original, en lugar de utilizar un borrado normal o formateado.

- **Sincronización de relojes.**
  Los relojes de los sistemas dentro de EPSA deben estar sincronizados con un tiempo acordado. Debe establecerse según una norma aceptada, por Ej. PST o un tiempo normalizado local.

4.10 Gestión de seguridad para la adquisición, desarrollo y mantenimiento de sistemas

Política de Adquisición, Desarrollo y Mantenimiento de sistemas

La Gerencia de Gestión de Tecnología debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento.

Estándares de la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

- **Requerimientos de seguridad de los sistemas.**
  La Gerencia de Gestión de Tecnología debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, consideren la administración de los riesgos de seguridad. Todos los requerimientos de seguridad se deben identificar durante la etapa de requerimientos, al igual que justificar, acordar y documentarse, como parte de todo el proyecto del sistema de información.

- **Seguridad de las aplicaciones del sistema.**

Se deben desarrollar estándares que indiquen cómo se deben asegurar los diferentes sistemas, aplicaciones y desarrollos, para minimizar la aparición de errores, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones.

Se deben diseñar controles adecuados en las aplicaciones, para garantizar un correcto procesamiento. Se debe incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes.

Las aplicaciones que se desarrollen en EPSA deben cumplir unos requerimientos mínimos de seguridad, conforme a las buenas prácticas en seguridad de la información y a esta política de seguridad. El diseño y operación de los sistemas debe obedecer a estándares de seguridad comúnmente aceptados y la normatividad vigente.

- **Seguridad de los sistemas de archivos.**
  Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del *software* aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.

- **Seguridad de los procesos de desarrollo y soporte.**
  Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control no estén comprometidos; igualmente deben cerciorarse de que los programadores de apoyo posean acceso sólo a las partes en el sistema necesarias para desarrollar su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

4.11 Cumplimiento y normatividad legal

Política para el Cumplimiento y Normatividad Legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

Estándares de la Política para el Cumplimiento y Normatividad Legal

- **Cumplimiento legal.**

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información de EPSA deben definirse previamente y documentarse de acuerdo con la metodología empleada por la empresa. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. El área jurídica de EPSA asesorará al Comité de Seguridad en dichos aspectos legales específicos.

- **Propiedad intelectual.**
  Se protegerá adecuadamente la propiedad intelectual de EPSA, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

- **Protección de datos.**
  Los estándares de seguridad son de obligatorio cumplimiento para los colaboradores con acceso a los datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:
  - Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
  - Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.
  - Funciones y obligaciones del personal con acceso a las bases de datos.
  - Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
  - Procedimiento de notificación, gestión y respuesta ante los incidentes.
  - Procedimientos de realización de copias de respaldo y de recuperación de los datos.
  - Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente.
  - Medidas a adoptar cuando un soporte o documento vaya a ser transportado, desechado o reutilizado.
  - El procedimiento se mantendrá actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

- **Cumplimiento de políticas y normas de seguridad.**
  Los gerentes de la compañía se deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluaran y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión con auditoria.

- **Cumplimiento técnico.**

Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deben realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad de la información, las vulnerabilidades y su grado de exposición al riesgo.

5. Documentación relacionada

- Código de Buen Gobierno Corporativo.
- Documentación del sistema de gestión.
- Política de Gestión Humana.
- Política de Gestión de Riesgos
- Política de tecnología de información y comunicación.

6. Definiciones

Para los propósitos de este documento, se definen los siguientes conceptos:

- **Activo:** cualquier cosa que tenga valor para la empresa.
- **Amenaza**: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Comité de Seguridad de la Información:** el Comité de Seguridad de la Información debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de la información de EPSA, aplicando los principios de confidencialidad, integridad y disponibilidad de la misma y de los recursos informáticos o de otra índole que la soportan, acorde con la planeación estratégica de la empresa.
- **Desastre o contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **EPSA:** se refiere a la EMPRESA DE ENERGIA DEL PACIFICO S.A. ESP, empresa de servicios públicos de carácter privado, con domicilio principal en la ciudad de Yumbo, y

cuyo objeto social principal comprende la realización de las actividades de generación, transmisión, distribución y comercialización de energía.

- **Estándares de seguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de *hardware, software* o infraestructura.

- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **Impacto:** la consecuencia que al interior de la empresa se produce al materializarse una amenaza.

- **Organización de seguridad:** es una función que busca definir y establecer un balance entre las responsabilidades y los requerimientos de los roles asociados con la administración de seguridad de la información.

- **Políticas:** toda intención y directriz expresada formalmente por la dirección**.**

- **Procesos:** se define un proceso de negocio como cada conjunto de actividades que reciben una o más entradas para crear un producto de valor para el cliente o para la propia empresa (concepto de cliente interno de calidad). Típicamente una actividad empresarial cuenta con múltiples procesos de negocio que sirven para el desarrollo de la actividad en sí misma.

- **Procedimientos:** los procedimientos son los pasos operacionales que los funcionarios deben realizar para alcanzar ciertos objetivos.

- **Riesgo:** combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*accountability*), no repudio y fiabilidad.

- **TI:** se refiere a tecnologías de la información
- **TIC:** se refiere a tecnologías de la información y comunicaciones
- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.