Instituto del Mar del Perú

Resolución Directoral DEC Nº 365-2015

Callao, 31 diciembre de 2015

VISTOS:

El Memorándum N° 526-2015-IMARPE-OGPP del 11 de noviembre de 2015; el Memorándum N°407-2015-IMARPE/OGPP del 14 de setiembre de 2015; el Informe N° AFIE-2015 del 21 de octubre de 2015 y el Informe N° OGAJ-317-2015 del 29 de diciembre de 2015.

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM del 22 de agosto del 2007, se aprobó el uso obligatorio de la Norma Técnica peruana NTP-ISO/IEC 17799:2007 "EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de dicha información;

C. AGUILAR

Que, la referida Norma Técnica Peruana indica que la Política de la Seguridad de la Información, tiene como objeto dirigir y dar soporte a la gestión de seguridad de la información en concordancia con los requerimientos de la institución, las leyes y regulaciones, correspondiendo a la Alta Dirección establecer las líneas de la políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una Política de Seguridad de la Información en todo la organización;

S. MIRANDA

Que, la Resolución Ministerial N° 129-2012-PCM del 23 de mayo de 2012, se aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 "EDI. Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos" en todas la entidades integrantes del Sistema Nacional de Informática, cuyo controles deberán ser implementados de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI. Tecnología de la Información;

R. CERRÓN

Que, mediante la Resolución Directoral N ° DEC-083-2015, del 25 de marzo de 2015, se conformó el equipo de trabajo denominado "Comité de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información – SGSI", como instancia administrativa responsable de dirigir, coordinar y revisar las puesta en práctica de la seguridad de la información del Instituto del Mar del Perú; teniendo como una de sus funciones, proponer políticas y normatividad de seguridad de la información para su aprobación;

H. SAENZ

Que, en ese sentido dicho Comité de Trabajo antes aludido, ha formulado el proyecto de "Política de Seguridad de la información en el Instituto del Mar del Perú", que tiene por objetivo establecer el marco general de gestión, para proteger adecuadamente la información y que se define como un conjunto de principios, lineamientos y responsabilidades para tal propósito;

De conformidad con lo dispuesto en el Decreto Legislativo N° 95, Ley del Instituto del Mar del Perú y su Reglamento de Organización y Funciones, aprobado por Resolución Ministerial N° 345-2012-PRODUCE;

Con la visación de la Secretaría General, Oficina General de Administración y del Área Funcional de Informática y Estadística y Oficina General de Asesoría Jurídica;

S. MIRANDA

R. CERRÓN

H. SAENZ

SE RESUELVE:

Artículo 1°.- Aprobar el documento de gestión interna denominado: "Política de Seguridad de la Información del Instituto del Mar del Perú" cuyo texto se presenta en anexo adjunto y que forma parte integrante de la presente Resolución Directoral.

Artículo 2°.- Se dispone que lo establecido en la "Política de Seguridad de la Información del Instituto del Mar del Perú" al que se refiere el artículo precedente, es de cumplimiento obligatorio por los funcionarios y servidores del Instituto del Mar del Perú.

Artículo 3°.- Disponer la publicación de la presente Resolución Directoral y su Anexo, en el Portal Institucional del Instituto del Mar del Perú (www.Imarpe.pe) y en el Portal de Transparencia.

Regístrese y comuníquese.

INSTITUTO DEL MAR DEL PERU
IMARPE

M.Sc. Carla P. Aguilar Samanamud
Directora
Dirección Ejecutiva Científica

Resolución Directoral DEC N° 365 -2015

Anexo

Política de Seguridad de la Información del Instituto del Mar del Perú

INDICE

PRESENTACION

I. OBJETIVO

II. ALCANCE

III. BASE LEGAL

IV. DISPOSICIONES GENERALES

V. PRINCIPIOS

VI. LINEAMIENTOS

VII. ROL Y RESPONSABILIDADES

VIII. GLOSARIO DE TERMINOS

PRESENTACION

"La Política de Seguridad de la Información en Imarpe", ha sido elaborada tomando como marco de referencia la Norma Internacional ISO/IEC 27001:2005, y la Norma Técnica Peruana NTP-ISO/IEC 27001:2008, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la institución.

Este documento institucional integra los lineamientos de las políticas de seguridad de la información e identifican las responsabilidades y establecen los objetivos para una protección adecuada y consistente de los activos de información del Instituto del Mar del Perú.

Las políticas de seguridad de la información que forman parte integrante del presente documento por sí solas no constituyen garantía para la seguridad de la información, sino que dependen principalmente de todo el personal tanto interno como externo para garantizar su cumplimiento.

El Instituto del Mar del Perú debe conducir un Sistema de Gestión de Seguridad de la Información, con el fin de establecer, operar, supervisar, revisar, mantener y mejorar la seguridad de la información en concordancia con las recomendaciones contenidas en las normas técnicas peruanas, estándares internacionales y mejores prácticas del SGSI.

I. OBJETIVO

El presente documento de gestión interna contiene la "Política de Seguridad de la Información del Instituto del Mar del Perú" que tiene por objetivo establecer el marco general de gestión para proteger de manera apropiada la Información del Imarpe para asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información y el fortalecimiento de una cultura de seguridad de la información de la entidad.

II. ALCANCE

El presente documento es de aplicación a:

- Personal del Instituto del Mar del Perú – Imarpe, sin distingo de régimen laboral o contractual o de nivel jerárquico
- Personas naturales o jurídicas que prestan servicios en general y/o que tengan acceso a la información del Imarpe.

III. BASE LEGAL

a) Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 13 julio de 2002.
b) Resolución Ministerial N° 246-2007-PCM del 22 de agosto de 2007, se aprobó el uso obligatorio de la Norma Técnica peruana NTP-ISO/IEC 17799:2007 "EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
c) Resolución Ministerial N° 129-2012-PCM del 23 de mayo de 2012, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 "EDI. Tecnología de la Información. Resolución Directoral N ° DEC-083-2015, que aprueba la conformación del equipo de trabajo denominado "Comité de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información – SGSI" en el Instituto del Mar del Perú.
d) Resolución de Contraloría General N° 320-2006-CG del 30 de octubre de 2006, que aprueba las Normas de Control Interno de aplicación en las entidades del estado.

IV. DISPOSICIONES GENERALES

Los Lineamientos se enmarcan en lo dispuesto por la Resolución Ministerial N° 129- 2012-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática, cuyo control deberá ser implementado de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información".

La información y los sistemas de información son activos importantes para el Instituto del Mar del Perú - Imarpe así como para la toma de decisiones de sus órganos.

La seguridad de la información, en su concepción moderna y técnica, busca, fundamentalmente, alcanzar los siguientes objetivos: confidencialidad, integridad y disponibilidad de la información en general.

4.1 Propiedad de la Información

Toda la información generada, almacenada y soportada por el Instituto del Mar del Perú - Imarpe, pertenece a la entidad y no puede ser utilizada en beneficio personal o de terceros.

4.2 Requisitos de Documentación

La documentación debe incluir registros de las decisiones de las unidades orgánicas del Imarpe, que asegure que las acciones realizadas respondan a las decisiones adoptadas y a las normas establecidas. La documentación del Sistema de Gestión de Seguridad de Información (SGSI) deberá incluir lo siguiente:

- Declaraciones documentadas de las normas y procedimientos que correspondan a la Seguridad de la Información.
- Alcance del SGSI.
- Metodología de Análisis de Riesgos
- Inventario de Activos
- Informe de evaluación del riesgo.
- Manual del SGSI
- Política del SGSI
- Declaración de Aplicabilidad
- Plan de tratamiento del riesgo.
- Plan de Trabajo para la Implementación de Controles
- Programa de Capacitación y Sensibilización
- Procedimientos documentados necesarios en la organización para garantizar la planificación efectiva, funcionamiento y control de sus procesos de seguridad de la información

V. PRINCIPIOS

Los siguientes principios constituyen los fundamentos sobre los que se basará cualquier acción en materia de la seguridad de la información:

a. Protección

Los activos de información deben ser protegidos con el nivel de seguridad adecuada, guardando proporción entre el valor y el riesgo de pérdida para el Imarpe. La protección debe enfocarse en la confidencialidad, integridad y disponibilidad de estos activos.

b. Uso apropiado

Los activos de información disponibles en el Imarpe deben ser utilizados en forma adecuada, eficiente, racional y exclusivamente para el desarrollo de las actividades institucionales.

c. Acceso autorizado

Todos los usuarios de los sistemas de información del Imarpe deben ser identificados individualmente, y sus permisos de acceso deben concederse en forma específica de acuerdo a su rol y responsabilidades. Los métodos de acceso a los usuarios deben exigir un proceso de autenticación, autorización y auditoría.

d. Disponibilidad

Los activos de información deben estar disponibles para su uso por parte de los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma.

e. Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad. Las medidas de validación definidas deben permitir detectar la modificación adecuada, adulteración o eliminación de los activos de información.

f. Confidencialidad

Los activos de información deben mantenerse protegidos para asegurar la confidencialidad y privacidad entre usuarios con acceso autorizado a los mismos. En todo momento deben mantenerse esquemas de seguridad que prevengan la divulgación no autorizada de información.

g. Colaboración

La conservación de la seguridad de la información es un esfuerzo de equipo en el que participan los trabajadores del Imarpe y terceros que tengan acceso a los activos de información del Instituto, por el cual estas personas deben desempeñar un papel activo en el cumplimiento y divulgación de las políticas y normas vigentes de seguridad de la información.

VI. LINEAMIENTOS

Los lineamientos de las políticas generales de seguridad de la información del Instituto del Mar del Perú - Imarpe son los siguientes:

6.1 Política de Seguridad de la Información

El presente documento de gestión interna que define la política y procedimientos asociados, debe ser cumplido por todo el personal del Imarpe y cualquier otra persona externa a la Institución que tenga acceso o interacción con la información de propiedad del Imarpe.

El Comité de Seguridad de Información debe monitorear el cumplimiento de la presente política, reportando los resultados a la Dirección Ejecutiva Científica al menos trimestralmente.

El Imarpe se reserva el derecho de tomar medidas disciplinarias indicadas en el Reglamento Interno de Trabajo o norma que corresponda al infractor, que falte a lo aquí dispuesto.

6.2 Organización de la Seguridad de la Información

El Imarpe debe mantener una organización interna que le permita prevenir, detectar y responder apropiadamente a eventos que pongan en riesgo la Seguridad de la Información. Para ello, es necesario que se defina en forma clara las responsabilidades del personal en relación con la Seguridad de la Información.

El presente documento establece los roles y funciones en el Imarpe para la gestión de Seguridad de la Información, a cargo del Comité de Seguridad de Información, Oficial de Seguridad de la Información, propietarios de la información y del personal del Imarpe.

6.3 Gestión de Activos de Información

El Imarpe debe elaborar y mantener un inventario de sus activos de información, asociados a cada proceso, sus propietarios y ubicación. El inventario será actualizado una vez al año o ante cualquier modificación de la información registrada; lo que suceda primero.

La responsabilidad de uso de los activos de información recae en el propietario de la información y de los procesos que manipula, sean estos manuales o electrónicos. Aunque tenga autoridad formal, no significa que tenga derechos de propiedad sobre el activo.

6.4 Seguridad de los recursos humanos

La seguridad de los recursos humanos, involucra a toda persona que utiliza la información del Imarpe para el desempeño de sus actividades y terceros que puedan tener acceso a información sensible.

Se debe verificar la idoneidad de las personas para prestar servicios en la entidad e incluir la suscripción de acuerdo de aceptación y cumplimiento de las Políticas de Seguridad de la Información para trabajadores del Imarpe y terceros que puedan tener acceso a la citada información.

Se deben realizar programas de concientización y entrenamiento para asegurar que los trabajadores del Imarpe asuman sus responsabilidades relacionadas con la seguridad de la información, estableciéndose procesos disciplinarios para casos de incumplimiento.

Al término de la vinculación laboral o contractual, debe asegurarse la devolución de activos asignados y el retiro de los derechos de accesos a los sistemas informáticos del Imarpe.

6.5 Seguridad física y ambiental

Las áreas e instalaciones de procesamiento, gestión o almacenamiento de información del Imarpe deben contar con mecanismos de control de acceso y protecciones físicas y ambientales apropiadas para prevenir el daño o pérdida de los activos de información.

6.6 Gestión de comunicaciones y las operaciones

Las actividades de gestión sobre los recursos de tecnología de información del Imarpe son esenciales para el buen funcionamiento de los servicios de esta Institución, se debe mantener documentados y actualizados los procedimientos operativos informáticos, controlar y documentar los cambios previamente autorizados sobre la plataforma tecnológica y efectuar una separación de tareas y áreas de responsabilidad.

Se deben aplicar medidas efectivas de protección para el software utilizado en los sistemas de cómputo, la información que estos procesan, y la información transmitida por sistemas de comunicación de datos en la red interna del Imarpe incluyendo el correo electrónico y los intercambios de información con cualquier entidad externa si los hubiera.

6.7 Control de acceso

Deben establecerse mecanismos para prevenir el acceso no autorizado a la bases de datos, sistemas de información, servicios de la red interna y plataforma de tecnología informática del Imarpe, así como garantizar la seguridad de la información de la entidad en entornos computacionales móviles.

Todo usuario autorizado debe poseer un identificador único para el acceso a los sistemas y servicios de información del Imarpe, debiéndose controlar la asignación

6.8 Adquisición, desarrollo y mantenimiento de sistemas de información

Se deben determinar los requisitos de seguridad para los nuevos sistemas de información del Imarpe o para los cambios de los sistemas informáticos existentes ya sean desarrollados internamente o por terceros, que incluyan las verificaciones del procesamiento correcto de las aplicaciones y la protección del código fuente y datos en producción.

Los nuevos sistemas a desarrollar y/o actualizar deberán cumplir el ciclo de vida de desarrollo de software, desde su requerimiento hasta la validación y aceptación formal por parte

de los usuarios solicitantes antes de su puesta en producción, respetando las normativas vigentes

Los cambios en las aplicaciones y en el ambiente de producción deben ser controlados adecuadamente, a fin de minimizar el riesgo en el procesamiento de la información.

6.9 Gestión de incidentes de seguridad de la información

Se deben establecer medidas para asegurar que las vulnerabilidades y eventos detectados que afectan negativamente a la seguridad de la información o procesos y/o actividades del Imarpe sean reportados, registrados y gestionados de manera que permitan la adopción de acciones preventivas y correctivas oportunas.

6.10 Gestión de la continuidad de negocio u operativa

El proceso de gestión de continuidad de negocio u operativa debe tomar en cuenta los aspectos necesarios para el tratamiento de los riesgos en seguridad de la información. Se debe contar con planes de continuidad operativa y contingencia que cubran los recursos informáticos e infraestructura tecnológica que dan soporte a los procesos principales del Imarpe, con la finalidad de garantizar la disponibilidad del servicio.

6.11 Cumplimiento de las normas legales y técnicas

Se deben establecer mecanismos para garantizar el cumplimiento de toda norma legal, directiva, regulación técnica u obligación contractual y de los requisitos de seguridad aplicables a los sistemas y activos de información del Imarpe.

VII. ROLES Y RESPONSABILIDADES

Para el cumplimiento de la presente Política de Seguridad de la Información en el Imarpe, se establecen las siguientes funciones:

7.1 Director(a) Ejecutivo(a) Científico(a)

El o la Director(a) Ejecutivo(a) Científico(a) del Imarpe a través del Comité demuestra su compromiso con el Sistema de Gestión de Seguridad de la Información y además debe:

a) Nombrar al Comité de Gestión de Seguridad de la Información del Imarpe.
b) Aprobar la Política y Objetivos de Seguridad de la Información, así como de su publicación y distribución. Asimismo, aprobar sus modificaciones con la asesoría del Comité de Gestión de Seguridad de la Información del Imarpe
c) Designar al Oficial de Seguridad de la Información.
d) Patrocinar el Sistema de Gestión de Seguridad de la Información (SGSI) del Imarpe
e) Delegar autoridad y responsabilidad a cada una de las Áreas, para el cumplimiento de la Política y Objetivos.
f) Comunicar la importancia de satisfacer los requisitos vigentes y aplicables al SGSI, en las diferentes reuniones.

g) Promover y Patrocinar la capacitación y concientización del personal del Imarpe en materia de seguridad de la información.
h) Asegurar la disponibilidad de los recursos (humanos, de infraestructura, financieros y tecnológicos), en el Plan Anual.

7.2 Comité de Gestión de Seguridad de la Información

a) Asegurar que se establezca y mantenga el Sistema de Gestión de Seguridad de la Información - SGSI de acuerdo a la Norma ISO/IEC 27001:2005 Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información - Requerimientos.
b) Informar al o a la Director(a) Ejecutivo(a) Científico(a) sobre el rendimiento del SGSI, para su revisión.
c) Dirigir y coordinar el avance y eficacia del SGSI en función a resultados de Objetivos, Metas y Auditorías Internas.
d) Revisar y proponer al o a la Director(a) Ejecutivo(a) Científico(a) para su consideración y aprobación, la política y las responsabilidades generales en materia de seguridad de la información.
e) Velar por el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.
f) Revisar y validar las normativas, procedimientos, estándares, metodologías y controles referidos a la seguridad de la información.
g) Identificar y canalizar los recursos necesarios para la gestión de la seguridad de la información.
h) Tomar conocimiento de los incidentes en materia de seguridad de la información de la entidad que se presenten, con el fin de evaluar la efectividad de los controles implementados.
i) Proponer planes y programas para mantener la conciencia en seguridad de la información.
j) Definir acciones a seguir en caso de situaciones no previstas que afecten la continuidad de los procesos críticos del Imarpe.
k) Revisar los procesos de auditoría interna y externa del Sistema de Gestión de Seguridad de la Información en forma periódica
l) Aprobar o proponer medidas a adoptar por el incumplimiento e infracciones a las políticas y normas de seguridad de la información.
m) Otras que considere necesario el o a la Director(a) Ejecutivo(a) Científico(a).

7.3 Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información será responsable de:
a) Elaborar propuestas y gestionar la aprobación de las políticas, normas, procedimientos y estándares relativos a la seguridad de la información del Imarpe.
b) Proponer al Comité y coordinar el análisis y evaluación de riesgos de los activos de información.
c) Supervisar el cumplimiento e implementación de las políticas, normas, procedimientos y controles referidos a la seguridad de la información.

d) Monitorear los cambios significativos en la infraestructura que puedan poner en riesgo los activos de información del Imarpe.
e) Monitorear la efectividad y eficiencia de los controles implementados para la protección de los activos de información.
f) Solicitar, efectuar o velar por el mantenimiento del SGSI.
g) Gestionar el control de los documentos del SGSI.
h) Solicitar, proponer y efectuar la administración de auditorías internas.
i) Efectuar el seguimiento de las acciones correctivas y preventivas.
j) Apoyar en la revisión por la Dirección del SGSI.
k) Promover y hacer seguimiento de la mejora continua de la aplicación de la Política de Seguridad de la Información.
l) Informar formalmente al Comité de Seguridad de la Información cualquier incidente o exposición de la información que represente un riesgo para la seguridad de la información.
m) Promover la difusión de una cultura en seguridad de la información al interior del Imarpe.
n) Dirigir la implementación y pruebas de los planes de contingencia.
o) Otros que considere necesario el Comité de Seguridad de Información.

7.4 Propietarios de la Información

Son responsables de:

a) Catalogar la información de acuerdo a los niveles de clasificación definidos.
b) Determinar los niveles de acceso que podrán tener los usuarios sobre la información.
c) Autorizar la asignación de accesos sobre la información.
d) Definir controles para la protección de los activos y asegurar su implementación.
e) Revisar periódicamente los accesos y privilegios otorgados sobre la información.
f) Velar por la integridad, confidencialidad y disponibilidad de la información.

7.5 Directores / Jefes

Los Directores / Jefes son responsables por:

a) Asegurarse que el personal a su cargo conozca y practique las políticas y normas de seguridad dispuesta en la entidad.
b) Asegurarse que la información y recursos bajo su control estén debidamente protegidos por las medidas de seguridad adecuadas.
c) Identificar los activos de información que manejan y las obligaciones individuales del personal a su cargo respecto a la seguridad de estos activos.
d) Asegurarse que el personal a su cargo tiene acceso solo a las aplicaciones y datos necesarios para realizar sus tareas.
e) Reportar inmediatamente al jefe inmediato superior y/o al Oficial de Seguridad el incumplimiento o infracciones a las políticas y normas de seguridad dispuestas mediante el presente documento.

7.6 Usuarios

Son responsables por:

a) Usar la información sobre la cual se les ha concedido acceso, solo para fines autorizados.
b) Cumplir con las medidas de seguridad establecidas en las políticas, normas y procedimientos de seguridad de la información.
c) Reportar inmediatamente al jefe inmediato superior y/o al Oficial de Seguridad cualquier trasgresión de las políticas y normas de seguridad dispuestas mediante el presente documento.
d) Usar los sistemas de información y la red solo para propósitos autorizados e inherentes a la función asignada.

VIII. GLOSARIO DE TERMINOS

a) **Activo de Información.-** Conocimientos o datos que tienen valor para el Imarpe

b) **Seguridad de la Información.-** Preservación de la confidencialidad, integridad y disponibilidad de la información.

c) **Sistema de Gestión de Seguridad de la Información (SGSI).-** Parte del sistema de gestión global, basada en un enfoque hacia los riesgos del negocio, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

d) **Riesgo de Seguridad de la Información.-** Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño al Imarpe.

e) **Integridad.-** Propiedad de salvaguardar la exactitud y completitud de los activos.

f) **Sistema de Gestión.-** Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos del Imarpe.

g) **Políticas.-** Intenciones globales y orientación como se expresan formalmente por la Dirección.

h) **Acción Preventiva.-** Acción adoptada para eliminar las causas de una no conformidad potencial u otra situación indeseable.

i) **Procedimiento.-** Forma específica, de llevar a cabo una actividad o un proceso.

j) **Registro.-** Documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

k) **Riesgo.-** Es la probabilidad que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos.

l) **Aceptación del Riesgo.-** Decisión de aceptar un riesgo.

m) **Análisis del Riesgo.-** Uso sistemático de la información para identificar fuentes y estimar el riesgo.

n) **Gestión del Riesgo.-** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.