ES COPIA AUTENTICADA

ROGER A. SICCHA MARTINEZ
Director General
Oficina General de Administración
MINISTERIO DE ECONOMÍA Y FINANZAS
06 FEB. 2015

Resolución Directoral

Lima, *06 de febrero de 2015* N° *037-2015-EF/43.01*

CONSIDERANDO:

Que, la Resolución Ministerial N° 129-2012-PCM, 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, cuyos controles deberán ser implementados de acuerdo a las recomendaciones 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. 2ª Edición", dispuesto por la Resolución Ministerial N° 246-2007-PCM;

Que, mediante Resolución Ministerial N° 649-2012-EF/10, se conformó el Grupo de Trabajo denominado "Comité de Gestión de Seguridad de la Información", como instancia administrativa responsable de dirigir, coordinar y revisar la puesta en práctica de la seguridad de la información en el Ministerio de Economía y Finanzas;

Que, la Resolución Ministerial N° 081-2014-EF/44, aprobó el documento de gestión interna denominado "Política de Seguridad de la Información del Ministerio de Economía y Finanzas", formulado por el Comité de Seguridad, en el marco de sus funciones establecidas en la Resolución Ministerial N° 649-2012-EF/10;

Que, asimismo el Comité de Gestión de Seguridad de la Información, en cumplimiento a sus funciones ha formulado y propuesto a la Oficina General de Tecnología de la Información, dos procedimientos relacionados al Sistema de Seguridad de la Información, denominados "Procedimiento de Revisión de la Política de Seguridad de la Información del Ministerio de Economía y Finanzas" y "Procedimiento de Gestión de Incidentes de Seguridad de la Información del Ministerio de Economía y Finanzas", para el respectivo trámite de aprobación.

Que, mediante Resolución Ministerial N° 223-2013-EF/41 se incorporó el numeral 5.5 en la Directiva N° 004-2012-EF/41.02 "Lineamientos para la Elaboración de Directivas en el Ministerio de Economía y Finanzas, aprobada con Resolución Ministerial N° 359-2012-EF/41, el cual establece que "La aprobación de Documentos Técnicos Normativos que no sean Directivas internas, tales como Manuales, Instructivos y otros de similar naturaleza, que emitan y propongan los órganos de administración interna del Ministerio de Economía y Finanzas, en materia de sus respectivas competencias, son aprobados por el Director General de la Oficina General de Administración";

J. Mvo. Odesada

Que, en ese sentido resulta necesario aprobar los procedimientos relacionados al Sistema de Seguridad de la Información, denominados "Procedimiento de Revisión de la Política de Seguridad de la Información del Ministerio de Economía y Finanzas" y "Procedimiento de Gestión de Incidentes de Seguridad de la Información del Ministerio de Economía y Finanzas", elaborado y propuesto por el Comité de Gestión de Seguridad de la Información, a través de la Oficina General de Tecnologías de la Información (OGTI) y en coordinación con la Oficina General de Planificación y Presupuesto;

De conformidad con lo dispuesto en la Resolución Ministerial N° 223-2013-EF/41, y en el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas, aprobado con Decreto Supremo N° 117-2014-EF;

SE RESUELVE:

Artículo 1.- Aprobar los procedimientos denominados "Procedimiento de Revisión de la Política de Seguridad de la Información del Ministerio de Economía y Finanzas" y "Procedimiento de Gestión de Incidentes de Seguridad de la Información del Ministerio de Economía y Finanzas", que como anexo forman parte integrante de la presente resolución.

Artículo 2.- Publicar la presente resolución en el Portal Institucional del Ministerio de Economía y Finanzas (www.mef.gob.pe), en el Intranet del Ministerio de Economía y Finanzas y disponer su difusión a todo el personal del MEF mediante correo electrónico.

Regístrese y comuníquese.

ROGER A. SICCHA MARTÍNEZ
Director General
Oficina General de Administración

PERÚ | Ministerio de Economía y Finanzas

PROCEDIMIENTO DE REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE ECONOMÍA Y FINANZAS

J.S.

Lima, octubre de 2014

CONTROL DE REVISIONES

Versión	Fecha de Revisión	Descripción de cambios en el documento
1.0	28.10.2014	Versión inicial de creación del procedimiento.

PROCEDIMIENTO DE REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE ECONOMÍA Y FINANZAS

1. OBJETO

Establecer las actividades necesarias para llevar a cabo la revisión de la Política de la Seguridad de la Información con el fin de asegurar su vigencia y efectividad en apoyo del Sistema de Gestión de Seguridad de la Información establecido en el Ministerio de Economía y Finanzas.

2. BASE LEGAL

2.1 Decreto Supremo Nº 117-2014-EF, que aprueba el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas.

2.2 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".

2.3 Resolución Ministerial Nº 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".

2.4 Resolución Ministerial Nº 246-2007-PCM, que aprueba 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. 2ª Edición".

2.5 Resolución Ministerial Nº 649-2012-EF/10, que conforma el Comité de Gestión de Seguridad de la Información del Ministerio de Economía y Finanzas.

2.6 Resolución Ministerial Nº 081-2014-EF/44, que aprueba el documento de gestión interna denominado "Política de Seguridad de la Información del Ministerio de Economía y Finanzas".

3. ALCANCE

El presente procedimiento alcanza a todos los miembros del Comité de Gestión de Seguridad de la Información constituido en el Ministerio de Economía y Finanzas para la conducción del Sistema de Gestión de Seguridad de la Información institucional.

4. DISPOSICIONES GENERALES

4.1 La revisión de la política de seguridad de la información debe realizarse por lo menos una vez cada dos años o en casos de cambios que la afecten, a fin de asegurar que siga siendo apropiada, conveniente y efectiva.

4.2 Para la revisión de dicha política se debe recopilar la información de apoyo necesaria como:

a) resultados de anteriores evaluaciones del riesgo en seguridad de la información;
b) informes de los órganos que podrían estar afectados en temas de seguridad de la información;
c) estado de las acciones preventivas y correctivas;
d) resultados de anteriores revisiones del Comité;
e) tendencias relacionadas con amenazas y vulnerabilidades;
f) incidentes reportados sobre seguridad de la información;
g) recomendaciones emitidas por autoridad competente, a nivel interno o externo.

4.3 Como resultado de la revisión puede establecerse la necesidad o no de cambios o mejoras en la política de seguridad de la información vigente. Las decisiones que se adopten, incluyendo la aprobación de una nueva política, se llevan a cabo y se documentan a través del Comité de Gestión de Seguridad de la Información mediante las sesiones de trabajo que se establezcan para el efecto.

4.4 El Coordinador de Seguridad de la Información proporciona todos los elementos técnicos y normativos al Comité de Gestión de Seguridad de la Información para el proceso de análisis, revisión y formulación de mejoras en la política institucional de seguridad de la información, de corresponder.

5. PROCEDIMIENTO

5.1 El Coordinador de Seguridad de la Información recaba la información requerida (leyes, normas, directivas, estudios, registros, estructura orgánica y otros) para evaluar las oportunidades de posibles mejoras de la Política de Seguridad de la Información del Ministerio.

5.2 Con la información obtenida el Coordinador de Seguridad de la Información evalúa si existen las condiciones por las que se amerita la revisión de la Política de Seguridad de la Información.

5.3 El Coordinador de Seguridad de la Información elabora un informe técnico sustentatorio de mejoras en la política de seguridad de la información, remitiéndolo al Presidente del Comité de Gestión para su conocimiento y revisión.

5.4 El Presidente del Comité de Gestión evalúa las consideraciones técnicas contenidas en el informe elaborado por el Coordinador de Seguridad de la Información y conjuntamente preparan la documentación necesaria para ser presentada ante el Comité de Gestión de Seguridad de la Información.

5.5 El Presidente del Comité convocará a una sesión de trabajo para evaluar la propuesta de revisión de la Política de Seguridad de la Información, remitiendo la documentación necesaria vía el correo electrónico institucional a los miembros del Comité de Gestión con una antelación de 48 horas.

5.6 Si se acuerda en el Comité de Gestión la conveniencia de la propuesta, se procederá a tramitar la aprobación y publicación de la Política de Seguridad de la Información actualizada y reformulada.

6. DISPOSICIONES COMPLEMENTARIAS Y FINALES

6.1 El Coordinador de Seguridad de la Información supervisará que las actividades descritas en el presente procedimiento se realicen de manera regular.

6.2 El presente procedimiento, una vez aprobado, entrará en vigencia a partir de la fecha de su publicación o difusión por el Comité de Gestión de Seguridad de la Información.

PERÚ | Ministerio de Economía y Finanzas

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE ECONOMÍA Y FINANZAS

Lima, noviembre de 2014

CONTROL DE REVISIONES

Versión	Fecha de Revisión	Descripción de cambios en el documento
1.0	20.11.2014	Versión inicial de creación del procedimiento.

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE ECONOMÍA Y FINANZAS

1. OBJETO

Establecer las disposiciones necesarias para el oportuno y adecuado tratamiento de los incidentes reportados en el Ministerio que se relacionan con la seguridad de la información, de manera que se minimicen los posibles daños a la información a cargo del Ministerio de Economía y Finanzas.

2. BASE LEGAL

2.1 Decreto Supremo Nº 117-2014-EF, que aprueba el Reglamento de Organización y Funciones del Ministerio de Economía y Finanzas.

2.2 Resolución Ministerial Nº 246-2007-PCM, que aprueba 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. 2ª Edición".

2.3 Resolución Ministerial Nº 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".

2.4 Resolución Ministerial Nº 649-2012-EF/10, que conforma el Comité de Gestión de Seguridad de la Información del Ministerio de Economía y Finanzas.

2.5 Resolución Ministerial Nº 081-2014-EF/44, que aprueba el documento de gestión interna denominado "Política de Seguridad de la Información del Ministerio de Economía y Finanzas".

2.6 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".

3. ALCANCE

El presente procedimiento es de cumplimiento obligatorio para el personal de los órganos y unidades orgánicas del Ministerio de Economía y Finanzas, cualquiera sea el cargo, función o actividad que realice e independientemente de su condición laboral o contractual.

4. DEFINICIONES

4.1 Asistencia al Usuario: función general de atención a las solicitudes de ayuda de los usuarios del MEF, incluyendo la recepción de notificaciones sobre incidentes o potenciales incidentes que pudieran afectar la seguridad de la información.

4.2 Evento de seguridad de la información: ocurrencia o cambio en el estado observado de un sistema, servicio o red, que constituye indicio de posible infracción de una política de seguridad de la información, falla de alguna protección o una situación previamente desconocida que pueda tener importancia para la seguridad.

4.3 Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información que tiene una probabilidad significativa de poner en peligro la integridad, disponibilidad y/o confidencialidad de la información.

4.4 Gestión de los incidentes de seguridad.- Conjunto de acciones para eliminar o mitigar los efectos de actos realizados o que pudieran realizar personal del MEF o terceros, orientados a afectar o que constituyan riesgos evidentes o potenciales que pudieran afectar la información o la seguridad de la información. Denominado también al Conjunto de Acciones correctivas o preventivas para lograr el mejoramiento continuo de la seguridad de la información.

5. DISPOSICIONES GENERALES

5.1 Para la gestión de los incidentes de seguridad de la información se adoptará un proceso de respuesta a incidentes de cuatro fases: preparación, registro y análisis, resolución, y revisión posterior al incidente.

5.2 La fase de preparación tiene como objetivo constituir una organización adecuada para responder de modo sistemático ante los incidentes de seguridad, así como establecer una capacidad de prevención de incidentes.

5.3 Durante la fase de registro y análisis se identifica y valida cada incidente reportado, se efectúa una evaluación inicial, se obtiene un diagnóstico de la situación y se documentan los hechos relevantes.

5.4 En la fase de resolución se toman decisiones de emergencia para erradicar el incidente y evitar su propagación, se recolectan evidencias y se investigan las causas del problema hasta establecer una solución definitiva, ejecutando finalmente las actividades de recuperación necesarias para retornar a las condiciones normales de operación.

5.5 A través de la fase de revisión posterior al incidente se procura mejorar las medidas de seguridad adoptadas y el desempeño del propio proceso de gestión de incidentes, realizando un análisis periódico de lo actuado que permita identificar las enseñanzas a recoger y las oportunidades de mejora.

5.6 El procedimiento aquí descrito puede integrarse dentro del proceso general de gestión de incidencias o de atención al usuario que se haya implantado en el Ministerio.

6. DISPOSICIONES ESPECÍFICAS

6.1 DE LA PREPARACIÓN

6.1.1 Se establecerá el grupo de trabajo especializado denominado Equipo de Respuesta a Incidentes de Seguridad con el propósito de coordinar

el manejo de los incidentes desde el momento de su notificación, estando conformado por personal de diferentes disciplinas con el cual se pueda gestionar la diversidad de problemas que puedan surgir como consecuencia de cada incidente en particular.

6.1.2 El Equipo de Respuesta a Incidentes de Seguridad estará integrado por:

a) El Coordinador de Seguridad de la Información, quien liderará el equipo;
b) Un especialista representante de la Oficina de Infraestructura Tecnológica de la Oficina General de Tecnologías de la Información (OGTI);
c) Un especialista representante de la Oficina de Sistemas de Información de la OGTI;
d) Un representante de la Oficina de Abastecimiento;
e) Un representante de la Oficina de Recursos Humanos;
f) Un representante de la Oficina de Seguridad y Defensa Nacional;
g) Un representante de la Dirección de Gestión de Riesgos.

6.1.3 La conformación del Equipo de Respuesta a Incidentes de Seguridad será solicitada a los correspondientes órganos del MEF, por el Presidente del Comité de Gestión de la Seguridad de la Información, una vez aprobado el presente procedimiento.

6.1.4 Los órganos y unidades orgánicas del Ministerio deberán brindar al Equipo de Respuesta a Incidentes de Seguridad todas las facilidades de acceso a la información requerida para el examen de los hechos y evidencias relacionadas con los incidentes de seguridad reportados.

6.1.5 En cada órgano o unidad orgánica del MEF deberá designarse un Delegado para la Seguridad de la Información, al cual el personal del área respectiva reportará cualquier incidente que considere esté relacionado a la seguridad de la información.

6.1.6 A fin de uniformizar los resultados del diagnóstico de los incidentes que se reporten, se establecerá un sistema de clasificación de incidentes que facilite la identificación, análisis, priorización y documentación de los mismos. En el **Anexo A** se muestra una tipología de incidentes de seguridad de la información que se utilizará inicialmente, pudiendo ser mejorada de acuerdo a la experiencia adquirida y a los resultados de las acciones de revisión y seguimiento de los incidentes.

6.1.7 Se proporcionará a los integrantes del **Equipo de Respuesta a Incidentes de Seguridad** el perfeccionamiento y entrenamiento que les permita adquirir y mantener el conocimiento y las destrezas necesarias para una efectiva actuación en el proceso de gestión de incidentes de seguridad de la información.

6.2 DEL REGISTRO Y ANÁLISIS

6.2.1 Cualquier trabajador del Ministerio debe reportar a la brevedad posible cualquier evento que haya observado y considere relacionado con la seguridad de la información, ante el Delegado para la Seguridad de su respectiva área a través de cualquier medio disponible para el efecto, sea teléfono, correo electrónico u otro.

6.2.2 El Delegado para la Seguridad evaluará, en primera instancia, el evento de seguridad reportado y de considerarlo pertinente comunicara al área responsable de la función de asistencia al usuario (tal como se define en el presente procedimiento) a través de cualquier medio disponible para el efecto, sea teléfono, correo electrónico u otro.

6.2.3 Se asignará un teléfono de emergencia o una persona de contacto disponible para los casos en que los canales habituales de atención de incidentes dejen de estar operativos.

6.2.4 El área responsable de la asistencia al usuario debe validar si el evento reportado es un incidente de seguridad o no. En caso de no serlo, finaliza el procedimiento de gestión de incidentes y el evento será atendido de acuerdo al proceso de soporte técnico al usuario que se haya establecido. En caso de validarse como incidente de seguridad se iniciará la gestión del mismo notificando al Equipo de Respuesta a Incidentes de Seguridad.

6.2.5 Las áreas técnicas de la OGTI deben identificar si los eventos detectados durante la ejecución de sus procesos de monitoreo de la infraestructura de TI resultan ser incidentes de seguridad. De ser cierto, se iniciará la gestión respectiva comunicando el hecho al Equipo de Respuesta a Incidentes de Seguridad.

6.2.6 El Equipo de Respuesta a Incidentes de Seguridad recopilará los datos relacionados con el incidente y los consignará en el Registro de Incidentes de Seguridad de la Información, cuya estructura se muestra en el **Anexo B**, procediendo luego al análisis del incidente identificado. Dependiendo de cada caso, la consignación de datos del incidente en el Registro podría realizarse en una etapa posterior de la gestión para permitir atender con prontitud las posibles urgencias.

6.2.7 Se comunicarán los incidentes de seguridad a los responsables de los activos de información afectados y a otros usuarios según se considere necesario, por cualquier medio de comunicación disponible para los efectos.

6.3 DE LAS ACCIONES DE RESOLUCIÓN

6.3.1 Según los resultados del análisis del incidente reportado de seguridad de la información, el Equipo de Respuesta a Incidentes de Seguridad coordinará y/o ejecutará las acciones de emergencia que se requieran para detener el impacto del incidente, o si la situación lo amerita, asegurará que se inicien las acciones establecidas en los planes de contingencia que sean aplicables.

6.3.2 El Equipo de Respuesta a Incidentes de Seguridad llevará a cabo una recolección de evidencias de cada incidente de seguridad para investigar la causa raíz correspondiente, registrando la información de dichas evidencias en el Registro de Incidentes de Seguridad de la Información.

6.3.3 El Equipo de Respuesta a Incidentes de Seguridad investiga las causas del incidente, determina una solución que se considere adecuada para resolver el incidente o prevenir futuras ocurrencias, asegura que se implemente la solución establecida y cierra el incidente. Las causas y la solución deben ser registradas en el Registro de Incidentes de Seguridad de la Información.

6.3.4 Cuando el incidente de seguridad no pueda ser resuelto internamente, se debe recurrir a los contactos de cooperación para estos casos (entidades del sector o afines) o asesores externos en seguridad de la información si las consecuencias del incidente lo ameritan. Con el apoyo de tales contactos de cooperación o asesores, se deben continuar las acciones de investigación y solución señaladas en el párrafo precedente, hasta que se logre solucionar el incidente.

6.3.5 Una vez que el incidente haya sido solucionado y cerrado, se deberá comunicar los resultados al usuario que reportó el incidente y a los afectados por el mismo, confirmando su solución efectiva.

6.4 DE LA REVISIÓN POSTERIOR AL INCIDENTE

6.4.1 El Equipo de Respuesta a Incidentes de Seguridad deberá efectuar una revisión del incidente cerrado en un lapso no mayor de una semana posterior al cierre, para examinar las acciones que se realizaron y determinar su efectividad, analizar los patrones de comportamiento del incidente e identificar las evidencias de debilidades y factores de exposición a riesgos que requieren ser atendidos para mejorar el desempeño de la gestión.

6.4.2 El Equipo de Respuesta a Incidentes de Seguridad mantendrá una bitácora de incidentes de seguridad en la que se compilarán los incidentes ya tratados con la estructura de datos indicada en el **Anexo C**, de manera que un análisis periódico de dicha bitácora permita reconocer las oportunidades de mejora según las tendencias que puedan observarse.

6.4.3 Se efectuarán revisiones de la bitácora de incidentes y los detalles individuales contenidos en el Registro de Incidentes con el fin de cuantificar y monitorear los tipos, volúmenes e impactos de los incidentes registrados históricamente. Para ello, se realizarán las siguientes acciones:

a) El Coordinador de Seguridad de la Información debe convocar al Equipo de Respuesta a Incidentes de Seguridad para una reunión de revisión de la bitácora de incidentes de seguridad, cuando se considere conveniente o con una periodicidad mínima anual.

b) En la reunión indicada se debe proceder con la revisión caso por caso de los incidentes registrados y determinar las respectivas lecciones aprendidas. Esta revisión debe estar orientada a identificar los incidentes más recurrentes y proponer la manera de prevenirlos eficazmente.

d) Se deben establecer las soluciones factibles a los problemas identificados que implican la adquisición de bienes o servicios, de manera que puedan ser sugeridas para el presupuesto de seguridad de la información del año entrante.

e) El resultado de esta revisión debe ser un informe de recomendaciones emitido por el Coordinador de Seguridad de la Información, quien lo elevará hacia el Comité de Gestión de Seguridad de la Información y/o hacia otros órganos del MEF según sea requerido.

7. RESPONSABILIDADES

7.1 Todo personal del MEF con acceso otorgado a documentos sensibles, equipos, recursos e instalaciones de procesamiento de información y comunicaciones son responsables de reportar cualquier violación actual o potencial de la seguridad de la información de acuerdo al presente procedimiento.

7.2 Las áreas técnicas de la OGTI son responsables de investigar, informar y tomar acciones apropiadas para tratar las violaciones a la seguridad de los sistemas informáticos y de las redes, así como reportar los incidentes al Coordinador de Seguridad de la Información y al Equipo de Respuesta de Incidentes de Seguridad.

8. DISPOSICIONES COMPLEMENTARIAS Y FINALES

8.1 El Coordinador de Seguridad de la Información supervisará que las actividades descritas en el presente procedimiento se realicen de manera regular.

8.2 El presente procedimiento entrará en vigencia a partir de la fecha de su respectiva aprobación por el Comité de Gestión de Seguridad de la Información.

ANEXO A

Tipología de Incidentes de Seguridad de la Información

Relación inicial, no limitativa, de tipos de incidencias relacionadas con la seguridad de la información:

- Uso indebido de información crítica (información reservada y/o relevante o de gran importancia para los objetivos misionales de la institución).
- Uso prohibido de un recurso informático o de red de la institución.
- Divulgación no autorizada de información personal.
- Intrusión física.
- Destrucción no autorizada de información.
- Robo o pérdida de información.
- Interrupción prolongada en un sistema o servicio de red.
- Modificación, instalación o eliminación no autorizada de software.
- Phishing (intentar adquirir información confidencial de forma inapropiada).
- Modificación no autorizada de un sitio o página web de la institución.
- Eliminación insegura de información.
- Modificación o eliminación no autorizada de datos.
- Anomalía o vulnerabilidad técnica de software.
- Amenaza o acoso por medio electrónico.
- Ataque o infección por código malicioso (virus, gusanos, troyanos, otros).
- Robo o pérdida de activos de información de la institución.
- Otro no contemplado.

ANEXO B

Registro de Incidentes de Seguridad de la Información

	REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Código:	
		Versión:	
		Fecha:	

Fecha de Notificación		Hora de Notificación	
DATOS DEL PERSONAL QUE NOTIFICA EL INCIDENTE			
Nombre y Apellido			
Teléfono			
E-mail			
Sede			
Gerencia			

INFORME SOBRE INCIDENTE			
Fecha en que observó el incidente		Hora en que observó el incidente	

Marque con una cruz todas las opciones que considere aplicables

	Uso indebido de información crítica		phishing (intentar adquirir información confidencial de forma
	Uso prohibido de un recurso informático o de red de la Institución		Modificación no autorizada de un sitio o página web de la Institución
	Divulgación no autorizada de información personal		Eliminación insegura de información
	Intrusión física		Modificación o eliminación no autorizada de datos
	Destrucción no autorizada de información		Anomalia o vulnerabilidad técnica de software
	Robo o pérdida de información		Amenaza o acoso por medio electrónico
	Interrupción prolongada en un sistema o servicio de red		Ataque o infección por código malicioso (virus, gusanos, troyanos, otros)
	Modificación, instalación o eliminación no autorizada de software		Robo o pérdida de activos de información de la Institución
	Acceso intento de acceso no autorizado a un sistema informático		Otro no contemplado.

INFORMACIÓN SOBRE EL INCIDENTE

Realice una breve descripción de la forma en la que descubrió el incidente:(cómo lo descubrió, si utilizó alguna herramienta, si conoce las fuentes del ataque o cualquier información pertinente):

Si el Incidente:

- Se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus.
- Se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla.
- Se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el oficial de Seguridad

INFORMACIÓN SOBRE EL ACTIVO AFECTADO		
Tipo de Activo		
Nombre del activo		
Descripción del Activo(S)		
Localización física:		
Describa brevemente la información contenida en el sistema / Computador:		
¿ Existe copia de respaldo de los datos o software afectado?	SI	NO
¿El recurso afectado tiene conexión con la red de la empresa?	SI	NO
¿El recurso afectado tiene conexión a Internet?	SI	NO

ANEXO C

Bitácora de Incidentes de Seguridad de la Información

Item	Fecha del incidente	Código de Incidente	Descripción del incidente	Tipo de incidente	Ubicación	Responsable	Datos de contacto del Responsable (teléfono, correo electrónico)	Recapitulación de acciones / Comentarios
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								