ANEXO XIV

CUMPLIMIENTO

1. OBJETIVOS

Garantizar el cumplimiento de las disposiciones legales, normativas y contractuales que sean de aplicación en la materia y promover el seguimiento y cumplimiento de las políticas, lineamientos y procedimientos de seguridad que se aprueben en el ámbito de la S.R.T..

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información, garantizando la existencia de controles que protejan los sistemas en producción y las herramientas de control en el transcurso de las auditorías de sistemas.

Atender y cumplir con las recomendaciones correspondientes a los hallazgos de las auditorías internas y externas que se realicen, adoptando las medidas correctivas que correspondan.

2. ALCANCE

Comprende a todo el personal de la S.R.T. cualquiera sea su modalidad de contratación y/o función que desempeñe como a todas las relaciones con terceros cualquiera fuere la vinculación con el organismo, abarcando, asimismo, a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del Organismo y a las auditorías efectuadas sobre los mismos.

3. DEFINICIONES

Registros: refiere a un tipo o conjunto de datos almacenados en un sistema en un espacio físico o virtual donde se deja constancia de un hecho, o el acto de hacer lo mismo.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) deberá identificar y documentar todos los requisitos normativos y contractuales pertinentes para cada sistema de información.

Asimismo, deberá verificar periódicamente que los sistemas de información cumplan con la política, lineamientos y procedimientos de seguridad establecidos en la presente resolución, y definir procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

Por otro lado, el RSI conjuntamente con la Subgerencia de Sistemas (S.S.) deberá realizar revisiones periódicas de todas las áreas de la SRT a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción.

La SS deberá tomar los recaudos necesarios en la planificación de los requerimientos y tareas que formen parte de las auditorías que se realicen sobre los sistemas de información.

Los Titulares de las Unidades Organizativas deberán supervisar el cumplimiento de la Política de Seguridad de la Información, así como con todos los documentos que de ella se desprendan, respecto de su personal, terceros vinculados a sus procesos y a la información que gestiona.

La Gerencia de Asuntos Jurídicos y Normativos (G.A.J. y N.) colaborará con el RSI cuanto este solicite asesoramiento acerca de los requisitos normativos y contractuales pertinentes para cada sistema de información en consonancia con las disposiciones legales vigentes en la materia.

La Unidad de Auditoría Interna verificará, a través de las auditorías que correspondan, el cumplimiento de la presente PSI.

5. CONTENIDO

5.1 CUMPLIMIENTO DE LEGISLACIÓN APLICABLE Y REQUISITOS LEGALES DE LOS SISTEMAS

5.1.1 Identificación y documentación de la legislación aplicable

Se deberán identificar y documentar los requisitos normativos, contractuales o legales que sean de aplicación respecto de los sistemas de información de la S.R.T..

Por otra parte, se deberá realizar una actualización periódica de los requisitos legales y contractuales para cada sistema de información, así como un relevamiento de la normativa de aplicación que pudiera tener impacto en la Política de Seguridad de la Información del Organismo.

5.1.2 Cumplimiento de la legislación aplicable y de la PSI

Se deberá supervisar el cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, así como de la Política de Seguridad de la S.R.T. y todos los documentos que de ella se desprendan.

5.1.3 Protección de los Registros de Datos

Los registros de datos de los sistemas de información de la S.R.T. que sean catalogados como críticos y aquellos que puedan requerir una retención segura para cumplir requisitos legales o normativos, se protegerán contra pérdida y/o destrucción y/o falsificación total o parcial.

5.1.4 Derechos de Propiedad Intelectual

Se implementarán medidas adecuadas para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

La S.R.T. solo podrá autorizar el uso de material producido por el mismo Organismo, o suministrado y autorizado por el titular del material, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

5.1.5 Protección de Datos y Privacidad de la Información Personal

Todo el personal de la S.R.T. deberá conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones.

Todo el personal suscribirá un compromiso con la S.R.T. por el cual se obligará a utilizar la información a la que acceda solo para el uso específico al que se ha destinado, teniendo en cuenta el no comunicar, diseminar, difundir o de alguna otra forma hacer pública la información a ninguna persona, sea física o jurídica, salvo autorización previa de un superior de nivel no inferior a Subgerente, y/o del Responsable de Seguridad de la Información, en el caso que lo amerite.

El documento a suscribir deberá informar sobre la existencia de actividades que por su criticidad y/o sensibilidad podrán ser objeto de monitoreo, en orden de resguardar el derecho a la privacidad del personal.

Asimismo, se deberá informar al personal sobre el cumplimiento y el alcance de las siguientes normas, y sus modificatorias, complementarias, y reglamentarias y/o en las que en el futuro las sustituyan:

NORMAS DE APLICACIÓN

A. Ley N° 20.744 “Contrato de Trabajo”
B. Ley Nº 24.156 “Administración Financiera y de los Sistemas de Control del Sector Público Nacional”
C. Ley N° 24.557 “Riesgos del Trabajo”
D. Ley Nº 24.766 “Confidencialidad sobre Información y Productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los Usos Comerciales Honestos”.
E. Ley N° 25.188 “Ética en el ejercicio de la Función Pública”
F. Ley Nº 25.326 “Protección de los Datos Personales”
G. Ley Nº 25.506 “Firma Digital”
H. Ley Nº 26.388 “Modificación del Código Penal – Incorporación de Delitos Informáticos”
I. Decreto Nº 41/99 “Código de Ética de la Función Pública”
J. Decreto N° 214/06 “Convenio Colectivo de Trabajo General para la Administración Pública Nacional”
K. Decisión Administrativa Jefatura de Gabinete de Ministros N° 641/2021 “Requisitos Mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional”
L. Disposición N° 1/2022 Dirección Nacional de Ciberseguridad “Modelo Referencial de Política de Seguridad de la Información”
M. Resolución S.R.T. N° 4/2019 “Estructura Organizativa de la S.R.T.”
N. Resolución S.R.T. N° 77/2020 “Creación del Comité de Seguridad de la Información”

5.1.6 Cumplimiento de los Sistemas de Información

La revisión periódica de los sistemas de información podrá incluir, entre otros, los siguientes procesos:

- Gestión de las vulnerabilidades
- Ciclo de vida de hardware y software
- Ciclo de vida de desarrollo

5.2 CONSIDERACIONES DE AUDITORÍA DE SISTEMAS

5.2.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se recomienda contemplar los siguientes aspectos:

A. Acordar los requerimientos de auditoría con las partes interesadas;
B. Definir el alcance de las verificaciones;
C. Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción;
D. Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores;
E. Proteger los elementos que se dispongan para su utilización en la auditoría.

5.2.2 Medidas correctivas sobre Auditorías de Sistemas

Se deberá considerar la adopción de las medidas correctivas que surjan a partir de las auditorías y revisiones periódicas de cumplimiento, sean estas realizadas por personal de la Unidad de Auditoría Interna, de Organismos competentes o de terceros habilitados a tal fin.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66589013-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO XIV Cumplimiento-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 5 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:42:15 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:56:38 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:56:39 -03:00