ANEXO II

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD

1. OBJETIVO

Contar con un marco organizativo que facilite una efectiva administración, gestión y operación de la seguridad de la información dentro de la S.R.T., para la implementación y control de los procesos relacionados con la seguridad de la información, así como para la distribución de funciones y responsabilidades.

Por otro lado, se pretende establecer mecanismos que permitan una adecuada seguridad cuando terceros, por diferentes circunstancias, tengan acceso a la información de la S.R.T..

2. ALCANCE

Comprende a todo el personal de la S.R.T. cualquiera sea su modalidad de contratación. Asimismo, se aplica a todas las relaciones con terceros que puedan tener acceso a la información, recursos y/o administración y control de los sistemas.

3. DEFINICIONES

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Es el cuerpo integrado en la S.R.T. destinado al tratamiento de temas relacionados a la Seguridad de la Información y a garantizar el apoyo manifiesto de las autoridades a las iniciativas en la materia.

MÁXIMAS AUTORIDADES: Se consideran como tal al Superintendente y Gerente General de la S.R.T..

4. RESPONSABILIDADES

El Comité de Seguridad de la Información (CSI) deberá garantizar el apoyo de las autoridades con relación al impulso de iniciativas de seguridad de la información del organismo. Asimismo, deberá revisar y proponer la Política de Seguridad de la Información (PSI) y las futuras actualizaciones que puedan presentarse.

Las Máximas Autoridades deberán asignar las responsabilidades relativas a la Seguridad de la Información (SI) a un área de la S.R.T. con competencias en la materia, promoviendo, en la medida de lo posible, la segregación de funciones para incrementar los niveles de seguridad.

Asimismo, deberán informar a la Dirección Nacional de Ciberseguridad los datos respecto al Responsable de Seguridad de la Información (RSI) asignado.

El RSI deberá elaborar la PSI y proponerla al CSI para su tratamiento.

El RSI deberá proponer la inclusión de aspectos para la identificación y análisis de riesgos desde el diseño y gestión de los proyectos del Organismo, que pudieran tener impacto en la seguridad de la información. Adicionalmente, se deberá contemplar al RSI en la gestión de proyectos, a efectos de garantizar que se reflejen adecuadamente las disposiciones de la Política de Seguridad de la Información en los mismos.

Por último, deberá garantizar el seguimiento de la PSI y su cumplimiento en el ámbito de la SRT.

La Subgerencia de Sistemas (S.S.) deberá implementar los aspectos de seguridad necesarios en la gestión de proyectos informáticos de acuerdo a lo establecido por el RSI. Asimismo, deberá implementar las medidas de seguridad establecidas sobre los dispositivos móviles y la modalidad de trabajo remoto, de acuerdo a la criticidad de la información involucrada y el nivel jerárquico del personal que la gestiona.

Los titulares de la Unidades Organizativas brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables dentro de sus dependencias.

Asimismo, en los casos que mantengan relaciones con terceros que puedan tener acceso a la información, recursos y/o administración y control de los sistemas, vinculados a través de contratos, convenios, acuerdos o demás instrumentos que plasmen dicha relación, serán responsables de gestionar la inclusión de cláusulas y su respectivo cumplimiento a sus obligaciones y responsabilidades en cuanto al cumplimiento de la Política de Seguridad de la Información y el deber de confidencialidad.

5. CONTENIDO

5.1 MARCO ORGANIZATIVO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Se deberá establecer un marco referencial organizativo, que permita gestionar y controlar la implementación de la seguridad de la información dentro de la S.R.T..

5.1.1 Compromiso de las máximas autoridades y Comité de Seguridad de la Información

Se deberá contar con un ambiente de gestión formalizado que garantice el tratamiento de las iniciativas de seguridad de la información ante las máximas autoridades, en pos de contar con su apoyo para impulsar las medidas necesarias.

El CSI funcionará como cuerpo integrado destinado a garantizar el apoyo de las autoridades y desde donde se impulsen y apoyen las iniciativas que se propongan con el objeto de preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona en el Organismo. Asimismo, se comprometerá con la seguridad de la información del Organismo a través de una orientación clara, proponiendo funciones generales en materia de Seguridad de la Información y asumiendo las responsabilidades establecidas en su conformación.

5.1.2 Asignación de responsabilidades de Seguridad de la Información

Se asignará a un área del organismo con competencia en la materia las responsabilidades relativas a la seguridad de la información, así como se promoverá, en la medida de las posibilidades, la segregación de funciones y de áreas de responsabilidad en conflicto para incrementar así los niveles de seguridad de la información.

Dicha área deberá tomar medidas tendientes a la separación de tareas, con el fin de evitar su concentración, prestando especial atención a las incompatibilidades existentes entre las funciones de un área específica, con respecto a las actividades desempeñadas por otras. Para el supuesto que, debido a la estructura y capacidad del área no se pueda dividir alguna de las funciones y se acumulen en el mismo personal varias actividades, se intentará compensar mediante la implementación de controles por oposición de intereses.

Asimismo, se deberá designar un Responsable de Seguridad de la Información (RSI) e informarlo a la Dirección Nacional de Ciberseguridad, así como también informar otros requisitos solicitados por esa Dirección.

Se deberán establecer responsables del cumplimiento de los distintos procesos de seguridad.

5.2 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LOS PROYECTOS DEL ORGANISMO

Se deberán implementar lineamientos que incluyan aspectos referidos a la seguridad de la información en el diseño y gestión de los proyectos que lleven a cabo dentro de la S.R.T..

5.3 DISPOSITIVOS MÓVILES Y TRABAJO REMOTO

Los dispositivos móviles provistos por la S.R.T., que pudieran gestionar información del Organismo, deberán cumplir con medidas seguridad adecuadas de protección de la información que contienen de acuerdo a la criticidad de la información involucrada y el nivel jerárquico del funcionario o personal al cual se encuentra asignado dicho dispositivo. Asimismo, se deberán contemplar lineamientos generales de seguridad para implementar en todo tipo de dispositivos, incluso personales, que pudieran ser utilizados para gestionar información relativa a la S.R.T..

Asimismo, se deberán establecer los criterios para la inserción de mecanismos de seguridad para la modalidad de trabajo remoto, cuando esta sea de aplicación.

5.4 ADMINISTRACIÓN INTERNA DE LA SEGURIDAD DE LA INFORMACIÓN

Se deberá velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos por la Política de Seguridad de la Información de la S.R.T.. Es por ello que se deberán realizar revisiones periódicas sobre la implementación y el cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables en todas las áreas del organismo.

5.4.1 Requisitos para terceros vinculados

Debe tenerse en cuenta que ciertas actividades de la S.R.T. pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información.

Por este motivo, es necesario que se establezcan cláusulas en los contratos, convenios, acuerdos o demás instrumentos para establecer y/o mantener dicha relación, que garanticen que los terceros vinculados con acceso a la información, recursos y/o administración y control de los sistemas, conozcan y acepten la PSI, así como cláusulas aplicables frente a su eventual incumplimiento.

Por su parte, se deberán incluir cláusulas y/o se solicitará la suscripción obligatoria de convenios de confidencialidad en los contratos, convenios, acuerdos o demás instrumentos para establecer relaciones con terceros.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan efectuado los controles apropiados, los cuales definan, asimismo, las condiciones para la conexión o el acceso, y se hayan suscripto los respectivos convenios respecto a la confidencialidad de la información.

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

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66575456-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO II Aspectos Organizativos de la Seguridad-EX-2023-56789749-APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 4 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:38:28 -03:00

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

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:43:36 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:43:37 -03:00