POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ARN

Contenido

1 INTRODUCCIÓN

La seguridad de la información requiere la implementación de un conjunto de controles, que abarquen políticas, prácticas, procedimientos, estructuras organizacionales, información en cualquiera de sus formas de almacenamiento, los aplicativos de software y sus funciones, entre otros controles. Esto permite que exista una gestión planificada en materia de seguridad, que atienda a las vulnerabilidades, a las fallas internas y a las posibles amenazas externas, sean deliberadas o accidentales, tales como intrusiones, ataques físicos y lógicos e incidencias que puedan ocurrir.

La Política recoge las medidas de seguridad establecidas con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de los sistemas de información y de los datos, cuando sean tratados por toda aquella persona humana y/o jurídica, funcionarios, trabajadores en el ejercicio de sus funciones, y aquellos prestadores de servicios y/o reparticiones públicas que la AUTORIDAD REGULATORIA NUCLEAR (ARN) requiera para cumplir sus objetivos.

2 OBJETIVOS DE LA AUTORIDAD REGULATORIA NUCLEAR

2.1 OBJETIVOS GENERALES

Dictar las definiciones operativas, los alcances organizativos y responsabilidades para el correcto manejo y utilización de los Sistemas de Información y los recursos asociados, acordes a las disposiciones legales y directrices vigentes con el fin de proteger los activos de información, frente a riesgos internos o externos, que pudieran afectarlos, para así preservar su confidencialidad, integridad y disponibilidad.

2.2 OBJETIVOS ESPECÍFICOS

Proteger la información, los datos personales y activos de información propios mediante un apropiado nivel de protección.

Promover una conducta responsable en materia de seguridad de la información de los organismos que conforman la AUTORIDAD REGULATORIA NUCLEAR (ARN), sus agentes y funcionarios.

Detectar, gestionar, prevenir y mitigar los riesgos e incidentes de seguridad, asegurando la continuidad de la seguridad de la información.

Evidenciar el compromiso e interés en pos del desarrollo de una cultura de Ciberseguridad.

3 ALCANCE

Todos los agentes y funcionarios de todas las actividades y sectores de la AUTORIDAD REGULATORIA NUCLEAR, incluyendo también a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

La Alta Dirección de la ARN será la responsable de proveer los medios necesarios para su efectivo cumplimiento y de promover su utilización.

4 DIRECTRICES

4.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ARN

Aprobada por la Alta Dirección de la ARN.

Notificada y difundida a todo el personal y a aquellos terceros involucrados cuando resulte pertinente y en los aspectos que corresponda.

Cumplida por todos los agentes y funcionarios del organismo.

Utilizada como base para establecer un conjunto de normas, procedimientos, lineamientos y guías acordes a los procesos que se llevan adelante en el organismo, su plataforma tecnológica y demás recursos de los que disponga.

Informada a la Dirección Nacional de Ciberseguridad una vez aprobada.

4.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD

Desarrollo e implementación de un marco organizativo que habilita una efectiva gestión y operación de la seguridad de la información en el organismo.

4.3 SEGURIDAD INFORMÁTICA DE LOS RECURSOS HUMANOS

Adoptar una perspectiva sistémica para proteger sus activos de información, considerando al personal como un recurso central.

Establecer una política de respeto de los derechos individuales de los empleados y resguardar su privacidad.

Concientizar y capacitar a los agentes y funcionarios para desarrollar habilidades y conocimientos en seguridad de la información, y hacer un uso responsable de la información y de los recursos utilizados en su gestión con el fin de prevenir riesgos.

4.4 GESTIÓN DE ACTIVOS

Gestionar y proteger en forma efectiva los activos de información del organismo. Clasificar según su criticidad para el organismo desde la perspectiva de su confidencialidad, integridad y disponibilidad, teniendo en cuenta sus funciones, la normativa que les sea aplicable y cualquier otro activo que pudieran contener de otros organismos públicos o entidades privadas, permitiendo adoptar las medidas de protección adecuadas.

4.5 AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESOS

Procesos y mecanismos de seguridad definidos e implementados según su nivel de criticidad, con el fin de proveer un nivel apropiado de protección. Los privilegios de acceso deben ser otorgados en forma expresa y formalmente autorizada a quienes los requieran para sus funciones.

4.6 USO DE HERRAMIENTAS CRIPTOGRÁFICAS

Proteger la información del organismo mediante técnicas de cifrado la confidencialidad, integridad, autenticidad y/o no repudio, tanto si los datos se encuentran almacenados como cuando son transmitidos.

4.7 SEGURIDAD FÍSICA Y AMBIENTAL

Proteger los activos de información del organismo mediante medidas que impidan accesos no autorizados, daños e interferencia, adoptando suficientes recaudos físicos y ambientales para minimizar los riesgos asociados.

4.8 SEGURIDAD OPERATIVA

Desarrollar en forma segura las operaciones del organismo, en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

4.9 SEGURIDAD EN LAS COMUNICACIONES

Proteger y controlar adecuadamente la información de las redes del organismo, tanto dentro de la organización como aquella que es transferida fuera de las instalaciones del organismo.

4.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Contemplar la seguridad de la información como una parte integral de los sistemas de información en todas las fases de su ciclo de vida, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet.

4.11 RELACIÓN CON PROVEEDORES

Incluir en la contratación, cualquiera sea la modalidad, realizada por el organismo para la provisión de un bien o servicio en el pliego de bases y condiciones particulares cláusulas de cumplimiento efectivo por parte del contratante, relacionadas con la seguridad de la información, desde el inicio del procedimiento contractual y hasta la efectiva finalización del contrato.

4.12 GESTIÓN DE INCIDENTES DE SEGURIDAD

Adoptar las medidas necesarias para prevenir, detectar, gestionar, resolver y reportar los incidentes de seguridad que puedan afectar sus activos de información.

4.13 ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN

Contemplar los procedimientos de continuidad de la gestión del organismo ante la ocurrencia de eventos de crisis o aquellos no planificados que impidan seguir operando en las instalaciones habituales todos los aspectos de seguridad de la información involucrada.

4.14 CUMPLIMIENTO

Cumplir con las disposiciones legales, normativas y contractuales que le sean aplicables, con el fin de evitar sanciones administrativas y/o legales y que los empleados incurran en responsabilidades civiles o penales como resultado de su incumplimiento.

5 REVISIÓN Y ACTUALIZACIÓN

La revisión de la Política de Seguridad de la Información será de forma anual, con una periodicidad no superior a DOCE (12) meses y de ser necesario se revisará y actualizará ante cambios significativos. Dicha revisión será realizada por el Comité de Seguridad de la Información y su actualización quedará a cargo del Responsable de Seguridad de la Información.

6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD

Conformación del Comité de Seguridad de la Información:

Con el objeto de impulsar los procesos necesarios para establecer un Sistema de Gestión de la Seguridad de la Información y procurar la homogeneidad de criterios para la inclusión estratégica de la seguridad de la información en todos los proyectos de la Institución, el Directorio de la Autoridad Regulatoria Nuclear, conforma el Comité de Seguridad de la Información, integrado por los siguientes Gerentes, Subgerentes y Jefes de Unidad del Organismo:

RESPONSABLE ACTIVIDAD SISTEMAS DE LA INFORMACIÓN
RESPONSABLE SISTEMAS INFORMÁTICOS
JEFE DE LA UNIDAD DE CALIDAD
GERENTE DE SEGURIDAD RADIOLÓGICA, FÍSICA Y SALVAGUARDIAS
GERENTE DE LICENCIAMIENTO Y CONTROL DE REACTORES NUCLEARES
GERENTE DE MEDICIONES Y EVALUACIONES EN PROTECCIÓN RADIOLÓGICA
SUBGERENCIA INTERVENCIÓN EN EMERGENCIAS RADIOLÓGICAS Y NUCLEARES
GERENTE DE ASUNTOS JURÍDICOS
GERENTE DE RECURSOS HUMANOS

Este Comité tendrá entre sus funciones:

- Revisar y proponer a la máxima autoridad del Organismo para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Actualizar la Política de Seguridad de la Información, al menos una vez al año o cuando ocurran cambios significativos a la Política adoptada.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación informática del Organismo.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

Coordinador del Comité de Seguridad de la Información

Designado por la Alta Dirección de la ARN

Coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y el cumplimiento de la presente Política.

Responsable de la Actividad Seguridad de la Información

Se designa en el ámbito de la Secretaria General, sin dependencia del Sector de Sistemas Informáticos.

Se notifica a la Dirección Nacional de Ciberseguridad, los datos de contacto.

Es responsable de Seguridad de la Información, tiene a su cargo las funciones relativas a la seguridad de los sistemas de información del Organismo.

Implementa, revisa y da cumplimiento a la Política de Seguridad de la Información.

Actúa como enlace con la Dirección Nacional de Ciberseguridad de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.

Informa y asesora al Comité de Seguridad de la Información, sobre la gestión del Sistema de Seguridad de la Información.

Gestiona los riesgos e incidentes de seguridad asociados a los activos de la información.

Obtiene resultados para determinar el tratamiento y prioridad de los riesgos identificados y los controles de seguridad a aplicar para mitigarlos.

Recibe las notificaciones de los incidentes de seguridad de la información, detectados e identificados y los comunica a la Dirección Nacional de Ciberseguridad, dentro de las 48 hs.

Recopila datos de las Unidades Organizativas, para valoración de riesgos.

Recibe pedidos de los distintos sectores de la Institución, para incrementar la seguridad de la información, según se incorporen Sistemas o contraten servicios nuevos.

Participa en el Plan de Contingencia para la continuidad de la seguridad de la información, ante incidentes o interrupciones imprevistas, en la operación de los Sistemas de Información Crítica y los Servicios Esenciales que presta el Organismo.

Responsable de Sistemas Informáticos

Supervisa todos los aspectos de seguridad informática asociados a la seguridad de la información.

Informa periódicamente al responsable de la Seguridad de la información y al Secretario General, al respecto.

Recibe las denuncias o evidencias sobre compromisos en la seguridad informática y actúa en consecuencia, informando al responsable de la Seguridad de la información y al Secretario General.

Monitorea y/o desconecta de la red cualquier equipo informático que afecte la seguridad o la operación normal de la red hasta que se regularice la situación.

Asesora a las unidades organizativas sobre la seguridad informática aplicada a la información clasificada procesada en la dependencia.

Revisa y propone actualizaciones en la seguridad de la información de los sistemas informáticos de acuerdo al estado del arte en la materia, informando al Secretario General y al Comité de seguridad de la información para la evaluación.

Establece responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Da cumplimiento a lo solicitado por los responsables de las unidades organizativas, UGSS, al acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementa seguridad en los accesos de usuarios por medio de técnicas de identificación y autenticación.

Implementa Firma Digital para el manejo de la documentación, en los casos que corresponda.

Controla la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

Registra y revisa eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

En los casos que se utilicen dispositivos móviles e instalaciones de trabajo a distancia se deberá garantizar la seguridad de la información.

Minimiza los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analiza las consecuencias de la interrupción del servicio y toma las medidas correspondientes para la prevención de hechos similares en el futuro.

Lleva un log de acceso a la Red.

Asegura la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

Responsable de la Gerencia Recursos Humanos

Notifica a todo el personal las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

Comunica la presente Política a todo el personal, así como de los cambios que en ella se produzcan.

Genera y coordina tareas de capacitación en materia de seguridad de la información.

Implementa la suscripción a los compromisos de confidencialidad y notificaciones de responsabilidad que se dicten.

Responsable del Sector Compras

Comunica la presente Política a todo contratista, así como de los cambios que en ella se produzcan.

Implementa la suscripción a los compromisos de confidencialidad y notificaciones de responsabilidad que se dicten, en los Contratos, Órdenes de Compra y/o documentos que vinculen a la ARN con Contratistas.

Responsable de la Gerencia de Asuntos Jurídicos

Asesorar sobre el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación con los empleados y, en caso de existir, con los terceros, como, asimismo, el Organismo en lo que cabe a su responsabilidad en la guarda y/o tratamiento de los datos.

Unidad Gestión de la Calidad

Realización de auditorías internas, revisión periódica del cumplimiento de los requisitos de la presente Política y evaluar la adopción de medidas correctivas que surjan de las auditorias.

Sanciones previstas por incumplimiento

Las sanciones previstas por el incumplimiento de la presente política serán objeto de medidas disciplinarias en función de lo establecido en el Reglamento del personal de la ARN.

Dispositivos Móviles y Trabajo a Distancia

Se establecen los requisitos de seguridad para el uso de dispositivos móviles y el trabajo a distancia, para el acceso a los recursos del organismo y consideraciones para el uso fuera del organismo en ambientes desprotegidos.

Dispositivos móviles del Organismo

Los dispositivos móviles y/o removibles provistos por el Organismo, notebooks, teléfonos móviles, tablets, etc., que contengan información de la institución, deberán cumplir con medidas de seguridad adecuadas para proteger la información almacenada y el dispositivo, de los riesgos derivados del uso. Para tal fin se desarrollan procedimientos de protección, de acceso y utilización que abarquen los siguientes conceptos:

- La protección física necesaria.
- El acceso seguro a los dispositivos.

- La utilización segura de los dispositivos en lugares públicos.
- El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
- Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- Los mecanismos de resguardo de la información contenida en los dispositivos.
- La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia, debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención acerca de portar un equipo valioso.
- No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
- No poner datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al poseedor del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

- Revocación de las credenciales afectadas
- Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

Dispositivos móviles personales

El acceso de dispositivos móviles personales, notebooks, teléfonos móviles, tablets, etc. a la infraestructura informática del organismo, deberá ser evaluado por el sector Sistemas Informáticos y autorizado conjuntamente por Seguridad de la información y la Secretaria General.

Los dispositivos móviles y/o removibles personales, notebooks, teléfonos móviles, tablets, etc., deberán cumplir con medidas de seguridad adecuadas para proteger los recursos del organismo a los que accede. Para tal fin se desarrollan procedimientos de protección, de acceso y utilización que abarquen los siguientes conceptos:

- El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
- Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- Monitoreo de acceso.
- La protección contra software malicioso.

Trabajo a Distancia

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

La solicitud para el acceso en modalidad Trabajo a Distancia, la efectúa el responsable de la Unidad Organizativa, UGSS, a la que pertenece el usuario/a solicitante, Sistemas informáticos y Seguridad de la información conjuntamente verifican que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes, finalmente, autoriza el Secretario General.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

- La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
- El ambiente de trabajo remoto propuesto.
- Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
- La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
- Evitar la instalación / desinstalación de software no autorizado por el Organismo.

Los controles y disposiciones comprenden:

- Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.
- Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
- Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
- Incluir seguridad física.
- Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
- Proveer el hardware y el soporte y mantenimiento del software.
- Definir los procedimientos de resguardo y de continuidad de las operaciones.
- Efectuar auditoría y monitoreo de la seguridad.
- Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
- Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

7 SEGURIDAD INFORMÁTICA DE LOS RECURSOS HUMANOS

Capacitar y concientizar al personal durante todo el ciclo de vida de la relación laboral resulta fundamental para el desarrollo de habilidades y conocimientos en seguridad de la información, asegura que los usuarios conocen las amenazas y los riesgos, lo que les permite hacer un uso responsable de la información y los recursos utilizados para su gestión.

El responsable de la Gerencia de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

La Gerencia de Asuntos Jurídicos participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Se declara el compromiso de concientizar y capacitar al personal en el uso seguro y responsable de los activos de información, con capacitaciones periódicas con distintas temáticas, que incluirán aspectos de la seguridad de la información en los cursos de inducción para recursos humanos.

Se promueve el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información y desarrollo de software e infraestructura.

Se garantiza que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Se establece la obligatoriedad de la suscripción de actas o compromisos respecto a la seguridad de la información para todos los empleados del organismo, cualquiera sea su modalidad de contratación, teniendo en cuenta que las responsabilidades correspondientes pueden exceder la vigencia de la relación laboral.

Se incorpora a las responsabilidades de los puestos de trabajo las funciones y responsabilidades en materia de seguridad de la información con el objeto de reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y manejo no autorizado de la información.

Se asegura que la selección de nuevo personal (permanente, contratado, becario) tenga en cuenta además de los requerimientos habituales, las verificaciones específicas propias del lugar de trabajo de destino, en particular si allí se maneja información clasificada.

Se desarrolla y aplica en coordinación con la Gerencia de Asuntos Jurídicos, lo detallado en el "Anexo de la Resolución N° 122/09 – Régimen disciplinario para el personal de la ARN" que viole la Política de seguridad de la información establecida.

Asegurar en coordinación con el respectivo jefe de unidad que todos los agentes de la ARN y cuando sea pertinente, personal externo, reciban una adecuada capacitación y actualización periódica en materia de Seguridad de la Información.

8 GESTIÓN DE ACTIVOS

El Organismo debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos, discos externos, etc.), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Se clasifican los activos de información, en línea con el tipo y la importancia de la información que gestionan para el organismo.

Se lleva un inventario actualizado en el que se detallen los datos necesarios para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.

Se exige a todos los agentes y empleados la devolución de los activos de información en su poder al finalizar la relación laboral o cuando un cambio en las funciones lo requiera.

Se efectúa una destrucción segura de cualquier medio que pueda contener información o datos personales, en función de su nivel de criticidad, sobre la base de un procedimiento documentado, una vez que se haya catalogado como defectuoso o rezago.

9 AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESOS

Para impedir el acceso no autorizado a los sistemas de información se implementan procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos están documentados, comunicados y controlados en cuanto su cumplimiento. Se implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

El responsable de Seguridad de la Información estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar periódicamente la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría.

- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
    - determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
    - definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
- Definir un cronograma de depuración de registros de auditoría en línea.
- Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.
- Los responsables de las Unidades Organizativas, junto con el responsable de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El responsable de Sistemas Informáticos cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de “enrutadores”, “gateways” y/o firewalls adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades (logs) de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

El Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Se utiliza en todos los casos el principio de “necesidad de saber”, es decir que solo se otorguen privilegios de acceso en la medida en que sean requeridos para las actividades y tareas que cada empleado o funcionario debe llevar adelante.

Se hace una adecuada y oportuna gestión de las altas y bajas de cuentas de usuario y privilegios, coordinando con la Gerencia de Recursos Humanos y aquellas en las que el empleado se desempeña toda novedad que pudiera impactar en ellos.

Se realiza un seguimiento detallado sobre las cuentas con privilegios especiales.

Se revisa periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.

Se requiere a los agentes, funcionarios y demás usuarios un uso responsable de sus dispositivos y datos de autenticación, dejando sentado que se encuentra estrictamente prohibido compartirlos y que deben ser mantenidos seguros en forma permanente.

Se restringe y controlar la asignación y uso de derechos de accesos privilegiados.

Se limita y monitorea el acceso al código fuente de los programas.

10 USO DE HERRAMIENTAS CRIPTOGRÁFICAS

Se utilizan sistemas y técnicas criptográficas para la protección de la información almacenada y transmitida, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

El responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el responsable de Seguridad de la información definirá junto con el responsable de Sistemas Informáticos, los métodos de encripción a ser utilizados.

Asimismo, el responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.

Se requiere el cifrado de cualquier dispositivo del organismo que contenga información considerada crítica y cuando involucre datos personales, especialmente cuando este se lleve fuera de la institución.

Se protegen adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.

Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, dentro y fuera del ámbito del Organismo.
- Para el cifrado de dispositivos móviles.
- Para los certificados digitales de todos los sitios de Internet del Organismo.

Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el responsable de Seguridad de la Información.

11 SEGURIDAD FÍSICA Y AMBIENTAL

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo, evitando el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados y protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

El responsable de Seguridad de la Información, Sistemas Informáticos y los Propietarios de Información, definirán según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la presente Cláusula.
El responsable de Sistemas Informáticos asistirá al responsable de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación.

Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Organismo.

Los responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados del Organismo cuando lo crean conveniente.

El Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal del Organismo es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Se identifican y protegen las áreas seguras contra desastres naturales, ataques maliciosos o accidentales.

Se incorporan controles físicos de ingreso/egreso, con los respectivos controles de identificación, cronológicos y de funcionamiento asociados, en aquellas áreas donde se encuentren resguardados los activos de información.

Se registran los activos físicos que procesan información, indicando su identificación, localización física y asignación organizacional y personal para su uso.

Se adoptan medidas de seguridad para que el equipamiento sea ingresado o retirado del organismo con una autorización previa y habiéndose adoptado todos los recaudos del caso.

Se mantiene el cuidado de los puestos de trabajo, mediante mecanismos de bloqueo de sesión y escritorio despejado.

Se adoptan medidas para evitar la pérdida, daño, robo o el compromiso de los activos de información del organismo y la interrupción de sus operaciones.

Se protegen los cables eléctricos y de red que transporten datos o apoyen los servicios de información frente a interrupciones, interferencia o daños.

Se realiza el mantenimiento del equipamiento para contribuir a su disponibilidad e integridad continua.

Se adoptan medidas de seguridad para los activos informáticos que deben llevarse fuera del organismo, considerando los distintos riesgos de trabajar fuera de sus dependencias, en lo que hace al resguardo de la información y a la seguridad física de los dispositivos.

12 SEGURIDAD OPERATIVA

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

El responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El responsable de Sistemas Informáticos tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El responsable de Seguridad de la información junto con el responsable Sistemas Informáticos y el responsable Asuntos Jurídicos del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el responsable de Seguridad de la Información y el responsable de Sistemas Informáticos, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Se establecen las responsabilidades y los procedimientos para la gestión y la operación para todas las instalaciones de procesamiento de información.

Se revisa, monitorea y ajustan los requerimientos de capacidad desde la perspectiva de la seguridad de la información.

Se minimizan los riesgos de acceso o de cambios no autorizados en entornos productivos, separando los entornos de desarrollo, prueba y producción, en los casos que corresponda.

Se implementa un monitoreo continuo sobre la seguridad de los sistemas e infraestructuras que soportan las operaciones críticas del organismo.

Se protegen las instalaciones contra infecciones de código malicioso.

Se realizan copias de resguardo del software y la información con una periodicidad y modalidad acordes con su criticidad de los datos y con los procesos que se lleven a cabo, probándolas periódicamente y estableciendo un registro de las pruebas de restauración que permitan conocer quién participó del proceso, cuándo y cómo lo hizo y dónde se encuentra la copia.

Se lleva registro de todos los eventos de seguridad y se lo revisa periódicamente con el fin de detectar posibles incidentes.

Se mantiene un control estricto sobre el software y su integridad, en entornos productivos.

Se identifica y gestiona adecuadamente las vulnerabilidades, así como el proceso de gestión de actualizaciones de todo el software utilizado. En los casos que el mismo sea provisto por terceros, se cuenta con una política de actualización para evitar que se afecte la operación.

Se gestiona de manera apropiada los reportes de vulnerabilidades y recomendaciones de actualización.

Se registra y revisa periódicamente las actividades de los administradores y operadores.

13 SEGURIDAD EN LAS COMUNICACIONES

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Para garantizar el funcionamiento correcto y seguro de las instalaciones y medios de comunicación:

El responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El responsable de Sistemas Informáticos tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

El responsable de Seguridad de la información junto con el responsable de Sistemas Informáticos y el responsable de Asuntos Jurídicos del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

El responsable de Seguridad de la Información junto con el Responsable Sistemas Informáticos definirá las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Segregar las redes de operación y control
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.
- Dicha configuración será revisada periódicamente por el responsable de Seguridad de la Información.

El Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Se segregan, en la medida de las posibilidades, los grupos de servicios de información, usuarios y sistemas en las redes.

Se protege adecuadamente la información que se transfiera dentro del organismo y hacia cualquier entidad externa, incluyendo aquella que se transmita a través de servicios de correo electrónico.

Se exige el uso de la cuenta de correo electrónico institucional a todos los agentes y funcionarios del organismo para toda comunicación vinculada con sus funciones, informando los riesgos de este incumplimiento.

Se incluyen mecanismos que garanticen las transferencias seguras en los acuerdos de servicio celebrados, tanto para servicios internos como tercerizados.

Se incorporan acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades del organismo en todos los acuerdos que se suscriban.

Se incorporan acuerdos y cláusulas de confidencialidad y no divulgación cuando el organismo entienda que resulta conveniente para el tipo de información que trate.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

El responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El responsable de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el responsable de Seguridad de la Información definirá junto con el responsable de Sistemas Informáticos, los métodos de encripción a ser utilizados.

Asimismo, el responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El responsable de Sistemas Informáticos, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de su área que considere adecuado, cuyas responsabilidades se detallan en la presente cláusula. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Sector de Sistemas Informáticos propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El responsable del Sector Compras incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El responsable de Asuntos Jurídicos participará en dicha tarea.

Se especifican lineamientos de seguridad desde la fase inicial del proceso de adquisición o desarrollo de un sistema (seguridad desde el diseño), cuando el proceso de contratación sea gestionado por el propio organismo.

Se utiliza una metodología de desarrollo seguro, capacitando a los desarrolladores e incorporando cláusulas en las especificaciones técnicas de los pliegos de bases y condiciones particulares.

Se controlan los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción e incorporando efectivos controles cruzados o por oposición.

Se protegen los datos utilizados en las pruebas, evitando la utilización de bases de datos reales.

Se utilizan protocolos que garanticen la transmisión o enrutamiento adecuados que eviten la divulgación, alteración o duplicación no autorizadas de transacciones.

Se evalúa la seguridad de las aplicaciones antes de ponerlas productivas, especialmente aquellas que se gestionen a través de Internet.

Se protege la información gestionada por aplicaciones web contra la actividad fraudulenta y los incumplimientos contractuales y de las normas legales vigentes.

Se controla y supervisa el efectivo cumplimiento y las actividades realizadas por el contratante en aquellas contrataciones de bienes y servicios efectuadas por el Organismo.

15 RELACIÓN CON PROVEEDORES

Los proveedores del Organismo deben ser gestionados en lo que respecta a los aspectos de seguridad que tienen que ver con el establecimiento y el acuerdo de todos los requisitos de seguridad de la información del Organismo.

Establecer y mantener el nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

El responsable de Seguridad de la Información junto con el Propietario de la Información debe definir en función a la criticidad de la información, los requerimientos de protección en lo referente al acceso de la información de los proveedores durante todo su ciclo de vida con el Organismo.

Asimismo, todo responsable de las áreas legales, compras o que gestionen los contratos con proveedores, deben garantizar que en los mismos se definan y se acuerden los niveles de seguridad establecidos por el Organismo.

Se tiene consideración de aspectos vinculados con la identificación, análisis y gestión de riesgo desde el estudio de factibilidad de cualquier decisión de contratación de bienes y servicios bajo cualquier modalidad contractual.

Se considera el establecimiento e inclusión en el pliego de bases y condiciones particulares de todos los requisitos de seguridad de la información pertinentes, en los acuerdos que se suscriban con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura tecnológica al organismo.

Se realiza la supervisión y revisión por parte de los responsables asignados al proyecto de todos los niveles de seguridad acordados.

Se considera la inclusión de cláusulas para mantenimiento del nivel de servicio, especialmente en servicios de provisión crítica, que permitan mantener su disponibilidad.

Se considera la inclusión en el pliego de bases y condiciones de estipulaciones tendientes al cumplimiento de todas las normas legales y contractuales que sean aplicables.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

Los Organismos cuentan con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y a la Dirección Nacional de Ciberseguridad de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, antes de 48 hs.

Asimismo, el responsable de Seguridad de la Información y el área de Gestión de Recursos Humanos son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes a los empleados y contratados al inicio de la relación laboral.

El responsable de Asuntos Jurídicos participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Se identifican las debilidades en los procesos de gestión de información del organismo, de manera de adoptar las medidas que prevengan la ocurrencia de incidentes de seguridad.

Se cuenta con procedimientos de gestión de incidentes de seguridad documentados, aprobados y adecuadamente comunicados, de acuerdo a las áreas funcionales que considere necesarias.

Se adopta una estrategia clara de priorización y escalamiento, que incluye la comunicación a las áreas involucradas, autoridades y a las áreas técnicas.

Se instruye a los agentes para la prevención, detección y reporte de incidentes de seguridad, según las responsabilidades correspondientes.

Se notifica a la Dirección Nacional de Ciberseguridad de la ocurrencia de incidentes de seguridad, en un plazo no superior a CUARENTA Y OCHO (48) horas de su detección.

Se recopila la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, de corresponder, resguardando la cadena de custodia.

En el caso en que el incidente de seguridad hubiere afectado activos de información y hubiere comprometido información y/o datos personales de terceros, se informa públicamente tal ocurrencia.

17 ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

El responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información, junto a los responsables de Seguridad de la Información, Sistemas Informáticos cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

Los responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.

Se identifican los requisitos necesarios para cumplir todos los requerimientos de seguridad de la información ante un evento inesperado que impida seguir operando, con foco en los servicios esenciales que preste el organismo.

Se establece, documenta, implementa y mantienen los procesos, procedimientos y controles tendientes al mantenimiento de un nivel de continuidad de la seguridad de la información durante situaciones adversas.

Se verifica, revisa y evalúa a intervalos regulares los controles de continuidad de la seguridad de la información.

Se implementan mecanismos para proteger la disponibilidad de la información crítica y de las instalaciones utilizadas para su procesamiento durante situaciones adversas.

18 CUMPLIMIENTO

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

La Gerencia de Asuntos Jurídicos del Organismo, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

El responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir normas y 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.
- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.
- El responsable de asuntos Jurídicos del Organismo, con la asistencia del responsable de Seguridad de la Información cumplirán las siguientes funciones:
- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Se cumple con la identificación, documentación y actualización periódica de los requisitos legales y contractuales para cada sistema de información que utilice.

Se da cumplimiento a la Ley No 25.326 de Protección de los Datos Personales y sus normas reglamentarias y complementarias.

Se realiza la revisión periódica de los sistemas de información para verificar el cumplimiento de las políticas y normas de seguridad de la información del organismo.

Se efectúa la supervisión del cumplimiento de todos los requisitos de seguridad contenidos en la legislación aplicable, incluyendo las directrices del presente documento, y en las políticas y procedimientos del organismo, por parte de los responsables de cada área del organismo, respecto a su personal y a la información que gestiona.

Se considera la adopción de las medidas correctivas que surjan de auditorías y revisiones periódicas de cumplimiento de los presentes requisitos, sean estas realizadas por personal del área, de organismos competentes o de terceros habilitados a tal fin.

19 TÉRMINOS Y DEFINICIONES

Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad:** Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación:** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio:** Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información:** Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Clasificación de la Información

La información debe ser clasificada para indicar la necesidad, prioridad y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial.

Datos Sensibles

Son aquellos definidos en el contexto de la o las leyes 25326 y 24804 en lo que cabe a las personas o lo relacionado con actividad regulada por esta Autoridad Nuclear. Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. El Organismo redactará un “Acuerdo de Confidencialidad”, el cual debe ser suscrito por el personal que depende directa o indirectamente del organismo, incluyendo a los contratistas. La copia firmada del compromiso será retenida en forma segura por el Organismo.

Datos Críticos

Es aquella información cuya indisponibilidad puede afectar el normal funcionamiento de una organización, no todos los datos tienen la misma criticidad, este factor será definido por los responsables de los mismos a través del formulario Control de la información documentada.

Sistema de Información

Conjunto independiente de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según procedimientos.

Tecnología de la Información

Se refiere al hardware y al software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Propietario de la Información

Define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento, la probabilidad que ocurran y su potencial impacto en la operatoria del Organismo.

Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Responsable de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

Propietarios de la Información

Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada, definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

Sistemas Informáticos

Cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo.

Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología apropiada de ciclo de vida de sistemas, y que contemple la inclusión de medidas de seguridad en los sistemas, en todas las fases.

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2021-87937853-APN-SG#ARN

CIUDAD DE BUENOS AIRES
Viernes 17 de Septiembre de 2021

Referencia: Anexo I Política Seguridad de la Información

El documento fue importado por el sistema GEDO con un total de 25 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.09.17 15:46:07 -03:00

Maria Guadalupe Gonzalez Barreiro
Analista
Secretaría General
Autoridad Regulatoria Nuclear

Digitally signed by Gestion Documental Electronica
Date: 2021.09.17 15:46:08 -03:00