hiberus

Política de Organización de la Seguridad

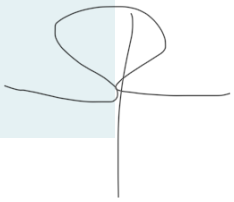
www.hiberus.com

Historial de cambios

Edición	Fecha	Modificaciones
1	10/09/2021	Creación documento
2	05/11/2023	Revisión terceros

Aprobación

Aprobación
Nombre: Sara Redondo **Cargo: Directora Dpto. Organización** **Fecha: 05/11/2023**



ÍNDICE

1. Generalidades 4
2. Objetivos 4
3. Políticas 4
3.1. Comité de Seguridad de la Información 4
3.2. Responsabilidades 5
3.3. Segregación de funciones 5
3.4. Seguridad de la información en la gestión de proyectos 6
3.5. Seguridad relacionada con terceros 6
3.6. Gestión de la entrega de servicios de proveedores 9

1. Generalidades

La presente Política de Seguridad de la Información establece la gestión de la seguridad de la información, como parte fundamental de los objetivos y actividades, tanto en instalaciones del Sistema de Información gestionadas por nosotros como en aquellas instalaciones gestionadas por nuestros clientes.

Por otro lado, debe tenerse en cuenta que ciertas actividades sobre los Sistemas de Información 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. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada gestión de seguridad, por lo que se establecerán las medidas adecuadas para su protección.

2. Objetivos

- Administrar la seguridad de la información dentro del Sistema de Información y establecer un marco gerencial para iniciar y controlar su implementación, así como para distribuir funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos a la información por parte de terceros.

3. Políticas

3.1. Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad compartida por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todas las áreas sustantivas y/o cliente y un Coordinador, quienes cumplirán la función de impulsar la implementación de la presente Política. En el caso del personal externo a nuestra empresa es una posibilidad su participación, no una obligación.

Este Comité de Seguridad de la Información tendrá entre sus funciones:

a) Revisar y proponer a la Alta Dirección para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

b) Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.

d) Planificar un análisis y evaluación de riesgos, mínimo cada año.

e) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

f) Presupuestar los recursos necesarios.

g) Elaborar un plan de formación y de sensibilización.

h) Sancionar las medidas de seguridad en el procesamiento de la información.

i) Planificar auditorías internas periódicas.

j) Supervisar y reportar a la Alta Gerencia sobre eventos e incidentes de seguridad.

k) Coordinar el proceso de gestión de la continuidad de operaciones de los sistemas de tratamiento de la información frente a interrupciones imprevistas.

3.2. Responsabilidades

La dirección deberá proveer evidencia de su compromiso con la seguridad de la información:

a) Establecer la Política de Seguridad.

b) Garantizar que los objetivos de seguridad de la información estén alineados a la dirección estratégica de la organización.

c) Establecer roles y responsabilidades.

d) Suministrar los recursos necesarios.

e) Decidir los criterios para aceptar el riesgo.

f) Garantizar que se ejecuten las auditorías internas.

g) Llevar a cabo revisiones gerenciales.

3.3. Segregación de funciones

Toda tarea en la que nuestro personal y/o colaboradores y/clientes tengan acceso a la infraestructura tecnológica y a los Sistemas de Información, deberá contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso o modificaciones no autorizados sobre los activos de información.

La gestión o ejecución de ciertas tareas o áreas de responsabilidad se separarán a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios, por falta de independencia en la ejecución de funciones críticas.

3.4. Seguridad de la información en la gestión de proyectos

Los requisitos de seguridad de la información deberán integrarse en la gestión de proyectos de implantación del Sistema de Información para asegurarse que los riesgos de seguridad de la información sean identificados y gestionados como parte del proyecto. Esto deberá aplicar a cualquier proyecto sin importar su carácter.
El método en gestión de proyectos en uso deberá:

a) Comprender los objetivos de seguridad de la información en los objetivos del proyecto.

b) Realizar una evaluación de riesgos de seguridad de la información en una primera etapa del proyecto para identificar los controles necesarios.

c) Incluir la seguridad de la información en cada una de las fases de la metodología aplicada en el proyecto.

d) Definir responsabilidades para la seguridad de la información y asignar a roles específicos definidos en los métodos de gestión de proyectos.

3.5. Seguridad relacionada con terceros

Se deberán definir normas y controles de seguridad que garanticen la adecuada y eficiente entrega de servicios por parte de proveedores e identificar los posibles riesgos de seguridad de la información con relación a los servicios que presta, así como establecer las correspondientes medidas de seguridad que ayuden a la mitigación de estos riesgos.
Cuando exista la necesidad de trabajar con terceros que requieran acceso al Sistema de Información y a la infraestructura donde éste se ubica, se deberá realizar una evaluación de riesgos para determinar las implicaciones para la seguridad y los requisitos de control.

Acceso a terceros

Cuando exista la necesidad de otorgar acceso al Sistema de Información por parte de terceros, el Dueño de los Riesgos de que se trate, llevará a cabo y documentará una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico y/o lógico y a qué recursos).
- Los motivos para los cuáles se solicita el acceso.
- El valor de la información.

- Los controles empleados por la tercera parte.

Todo acceso por parte de un tercero a los Sistemas de Información deberá ser autorizado por un responsable interno, quien asume la responsabilidad por las acciones que pueda realizar el mismo. En ningún caso se otorgará a terceros el acceso a la información, instalaciones de procesamiento u otras áreas de servicios críticos, hasta que se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

Acuerdos con terceros

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de nuestra empresa, se establecerán los controles, requerimientos de seguridad y acuerdos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.
Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.

b) Personal de limpieza, de seguridad y otros servicios de soporte tercerizados.

c) Servicio social y otras designaciones transitorias o de corto plazo.

d) Consultores.

Se revisarán los contratos o acuerdos existentes, o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de Seguridad de la Información relativa a los Sistemas de Información.

b) Protección de los activos de los Sistemas de Información, incluyendo:

- Procedimientos para proteger los activos físicos, la información y el software.
- Procedimientos para el intercambio de información.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los activos, como por ejemplo la pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.

Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Obligaciones y responsabilidades legales de las partes, emanadas del acuerdo o contrato.

e) Definiciones relacionadas con la protección de datos.

f) Acuerdos de control de acceso que contemplen:

- Métodos de acceso permitidos, el control y uso de identificadores únicos.
- Proceso de autorización de accesos y privilegios de usuarios.

g) Nivel de servicio esperado y niveles de servicio aceptables.

h) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

i) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

j) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

k) Proceso claro y detallado de administración de cambios y gestión de incidentes.

l) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

Cadena de suministro de TIC

Los acuerdos o contratos con proveedores deberán incluir requisitos que consideren los riesgos de seguridad de la información asociados con los servicios de tecnologías de la información y comunicación y cadena de suministro de productos, considerando entre otros aspectos:

a) Solicitar a los proveedores hacer extensivo los requisitos de seguridad de la organización a lo largo de la cadena de suministro si es que ellos subcontratan partes del servicio o producto.

b) Obtener garantía de que a la entrega de productos de TICs funcionarán como se espera sin alguna situación inesperada o no deseada.

c) Definir reglas para el intercambio de información relacionada con la cadena de suministro y cualquier asunto y compromiso entre la organización y los proveedores.

Implementar procesos específicos para la gestión del ciclo de vida y disponibilidad de componentes y riesgos de seguridad asociados.

3.6. Gestión de la entrega de servicios de proveedores

La entrega de los servicios de proveedores y el nivel de seguridad de la información acordado deberán estar alineados a los acuerdos previamente establecidos, considerando:

a) Monitorear los niveles de desempeño de los servicios para verificar la adherencia a los acuerdos.

b) Revisar los reportes de servicios elaborados por el proveedor y acordar reuniones de seguimiento de acuerdo con lo establecido en el acuerdo.

c) Resolver y gestionar cualquier problema identificado.

d) Asegurarse que los proveedores mantienen un nivel de capacidad suficiente para garantizar el cumplimiento de los niveles de continuidad de servicio en caso de una falla o desastre.

e) Gestionar cambios en la prestación de servicios por parte de los proveedores, teniendo en cuenta la criticidad de la información del negocio, los sistemas, los procesos involucrados y la reevaluación de los riesgos.

www.hiberus.com