GUÍA DE CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS PARA LA SEGURIDAD DE LA INFORMACIÓN

Bogotá D.C. 2022

Tabla de contenido

Indicador de tablas

1. Introducción

Capital Sistema de Comunicación Publica a través del Sistema de Gestión de Seguridad de la Información-SGSI opta por mantener contacto con las entidades y grupos de interés especializados en seguridad de la información debido al uso continuo de tecnologías de la información y las comunicaciones en todas las actividades que llevan a cabo sus colaboradores, contratistas y terceros.

Partiendo del conocimiento y la experiencia del Profesional Especializado de Sistemas, el Oficial de Seguridad de la Información y el Grupo de Soporte de la Entidad sobre los riesgos, amenazas y vulnerabilidades, se llevan a cabo diversas acciones encaminadas a la Seguridad de la Información y permiten formar de manera adecuada al personal de tecnología en la aplicación de procedimientos de seguridad.

Con la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de las TIC, conduce a la protección de la confidencialidad, integridad, disponibilidad y privacidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de su adecuado manejo.

2. Objetivo

Definir y asegurar que los colaboradores, contratistas y terceros de Capital tengan identificados los contactos adecuados para la gestión de la Seguridad de la Información, actualizaciones al Modelo de Seguridad y Privacidad de la Información, noticias de interés, incidentes de seguridad que requieran del acompañamiento de especialistas, autoridades y mayor escalamiento.

3. Alcance

Definir una guía con los datos de contacto con autoridades y grupos de interés, las cuales deben ser acatadas por cada uno de los colaboradores, contratistas y terceros que laboren o presten servicios para Capital, esto con el fin de dar cumplimiento adecuado a sus funciones, conocimiento y mantener un nivel de protección a la información.

4. Responsables

- Alta Gerencia.
- Profesional Especializado de Sistemas - Oficial de Seguridad de la Información.
- Profesional Especializado Área Técnica.
- Ingenieros de Soporte.
- Grupo de recursos Informáticos.
- Proveedores – Contratistas - Terceros.

5. Generalidades

Esta guía ofrece un lineamiento para la acción inmediata en cualquier caso de incidente con respecto a la seguridad de la información que pueda poner en peligro la confidencialidad, integridad y disponibilidad de la información de Capital. Cualquier violación de seguridad, debe ser reportado de manera inmediata por los canales dispuestos para este fin, los cuales evaluaran la acción que se debe tomar con los funcionarios o personal involucrado.

6. Autoridades y Grupos de Interés

A continuación, se informa de las autoridades dispuestas para este fin con respecto a la seguridad de la información en caso que se presente algún incidente, violación o eventualidad.

El Profesional Especializado de Sistemas con el rol de Oficial de Seguridad de la Información, será los encargados de tener contacto con las Autoridades y Grupos de Interés cuando se presenten incidentes que pongan en riesgo la Seguridad de la Información. Así mismo es el encargado de realizar transferencia de conocimientos a las áreas de Capital, también realizar el envío de consejos de seguridad en temas de información y tecnología.

	NOMBRE ENTIDAD	CONTACTO	INCIDENTE O EVENTUALIDAD
Autoridades	Centro Cibernético Policial CAI Virtual Policía Nacional. **(CCP)**	https://caivirtual.policia.gov.co/	• Acceso abusivo a sistemas informáticos. • Violación de datos personales • Uso de software malicioso • Suplantación de sitios web • Transferencia no consentida de activos • Hurto por medios informáticos • Ingenieria social
	Grupo de Respuestas a Emergencias Cibernéticas de Colombia. **(COLSERT)**	http://www.colcert.gov.co/	• Respuesta a emergencias cibernéticas de Colombia
	Centro de Coordinación Seguridad Informática de Colombia Policía Nacional. **(CSIRT-CCIT)**	https://cc-csirt.policia.gov.co/	• Atención a incidentes de seguridad informática colombiano
	Ministerio de las Tecnologías de la información y las Comunicaciones **MINTIC.**	https://www.mintic.gov.co	• Encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones
	Alta Consejería para las TIC – Gobierno Digital.	**http://ticbogota.gov.co/** **http://estrategia.gobiernoenlinea.gov.co**	• Lineamientos, directrices, estrategias e instrumentos para orientación con tecnologías públicas.

6.1 Tabla Autoridades - Seguridad de la Información

	NOMBRE ENTIDAD	NOMBRE CONTACTO CANAL CAPITAL	EMAIL Y TELÉFONO CONTACTO
Grupos de Interés	Centro Cibernético Policial CAI Virtual Policía Nacional. **(CCP)**	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Grupo de Respuestas a Emergencias Cibernéticas de Colombia. **(COLSERT)**	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Centro de Coordinación Seguridad Informática de Colombia Policía Nacional. **(CSIRT-CCIT).**	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Ministerio de las Tecnologías de la información y las Comunicaciones **MINTIC.**	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Alta Consejería para las **TIC** – Gobierno Digital.	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Comité de **G**estión y **D**esempeño de Capital	Mauris Antonio Avila Velásquez	**Tel:** (60 1) 4578300 ext 5000 **Email:** mauris.avila@canalcapital.gov.co
	Área de Sistemas Capital	Modulo soporte mesa de ayuda-Intranet o al correo del gestor de seguridad informática.	**INTRANET:** **https://intranet.canalcapital.gov.co/erp/** **Email:** Seguridad.informatica@canalcapital.gov.co

6.2 Tabla Grupos de interés – Seguridad de la Información

7. Documentación referencia

Modelo de Seguridad y Privacidad de la Información:

https://www.mintic.gov.co/gestionti/615/articles-482_Modelo_de_Seguridad_Privacidad.pdf

8. Glosario

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados.[1]
- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas…) que tenga valor para la organización.
- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.
- Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento.
- Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre

[1] Tomado del documento Modelo de Seguridad Privacidad de Mintic página 11. Disponible en la URL : https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

usuarios.

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural.
  Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- Información Pública Clasificada: Es aquella información que estando en poder o custodia

[2] Tomado del documento Modelo de Seguridad Privacidad de Mintic página 11. Disponible en la URL : https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

- Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.
- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.
- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
- Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- [3]Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos

[3] Tomado del documento Modelo de Seguridad Privacidad de Mintic página 11. Disponible en la URL : https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
[4] Tomado del documento Modelo de Seguridad Privacidad de Mintic pagina 11. Disponible en la URL : https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento.
- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.