1.- Sistema de Seguridad de la Información

Objetivo: Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información

¿Que es un activo de información?

Son todos aquellos documentos, bases de datos, sistemas y software de aplicación, personas, equipos informáticos, redes de transmisión de datos, datacenter, soportes de almacenamiento, y otros elementos de infraestructura que están sujetos a diferentes tipos de amenazas e inseguridades, tanto desde dentro de la propia organización como desde fuera de ella.

1.- Sistema de Seguridad de la Información

Responsabilidades: En caso de que se produzca un incidente de seguridad de la información se debe comunicar en forma inmediata con el Encargado de seguridad de la información del Servicio o reportarlo mediante la intranet en el Formulario de denuncias anónimas que se encuentra en la intranet.

http://intranet.gobiernosantiago.cl/denuncias

1.- Sistema de Seguridad de la Información

En caso de emergencias, ¿cuándo y a que numero llamar?

En caso de	Teléfono
Presencia de fuego con riesgo de propagación	132 Bomberos
Personas atrapadas en ascensores, maquinarias, inmuebles	
Colisión, choque o volcamiento de vehículos	
Derrame de elementos químicos	
Emanaciones de gases	
Accidentes eléctricos en la vía publica	
Accidentes aéreos en zona urbana	
Cumplimiento de la Ley y restauración del orden publico	133 Carabineros
Atención a víctimas en caso de accidentes, catástrofe o delitos	
Atención médica de urgencia	131 Ambulancia
En caso de intoxicación con medicamentos	26353800 Universidad Católica de Chile
Emergencias Eléctricas	26971500 Chilectra
Accidente del trabajo y/o enfermedades profesionales	26775000 Mutual de Seguridad **Rescate Emergencia** **1407 / 600 301 2222**

2.- Políticas para la seguridad de la información

El valor de la información traspasa las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas intangibles de información.

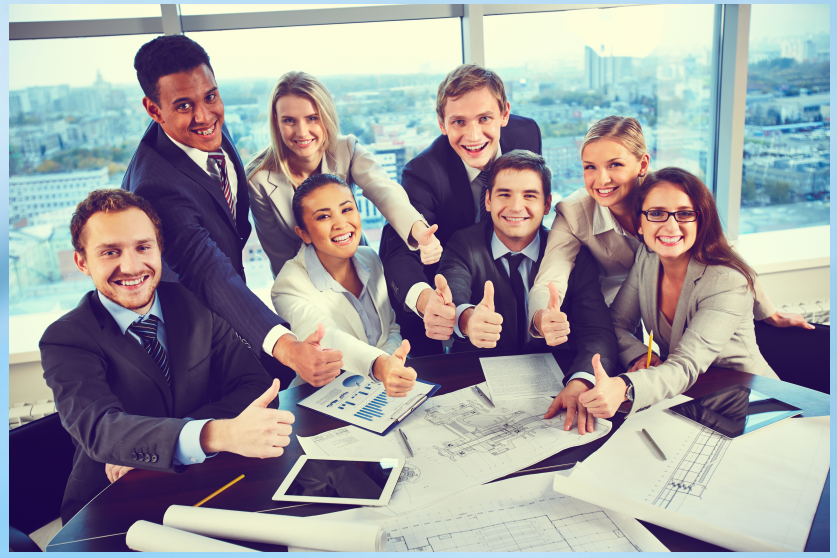
En un mundo interconectado, la información y los procesos relacionados, los sistemas, redes y el personal involucrado en su operación, manipulación y protección son activos que, al igual que otros activos comerciales de importancia, resultan valiosos para el negocio de la organización y, por lo tanto, merecen o requieren protección contra diversos peligros.

2.- Políticas para la seguridad de la información

Objetivo: dar orientación y apoyo en la administración para la seguridad de la información de acuerdo con los requisitos comerciales y las leyes y normativas pertinentes.

Productos: Las políticas internas son especialmente útiles en el Servicio, donde aquellos que definen y aprueban los niveles ampliados de control se segregan de los que implementan los controles o en situaciones donde una política se aplica a varias personas o funciones distintas de la organización.

2.- Políticas para la seguridad de la información



Difusión: Las políticas se deben comunicar a los Funcionarios y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un programa de Concientización, educación y capacitación sobre la seguridad de la información

3.- Revisión de las políticas del SSI

Control: Las políticas para la seguridad de la información se deben planificar y revisar en intervalos o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad continua.

Implementación: Cada política cuenta con un responsable administrativo cuya responsabilidad encargado de su desarrollo, Revisión y evaluación. La revisión debería incluir la evaluación de oportunidades de mejora en las políticas de la organización y un enfoque para administrar la seguridad de la información en respuesta a los cambios en el entorno organizacional, las circunstancias comerciales, las condiciones legales o el entorno técnico

4.- Política de Clasificación de activos

Objetivo: Mantener y alcanzar una apropiada protección de los activos.

Alcance: Permitir la correcta identificación y etiquetado de los activos provistos en el Gobierno Regional, indicando la importancia que los activos tienen.

Inventario de activos: Identificar los activos y la importancia de estos para el Servicio.

4.- Política de Clasificación de activos

Clasificación de la información

Información Pública: Son los activos de *información que no contienen datos sensibles* que pudiera afectar la integridad de los procesos y/o las personas.

Información Confidencial: Aquella *información con datos sensibles* que pudiera afectar la integridad de los procesos y/o las personas.

****Mas información indicada en Ley 20.285****

4.- Política de Clasificación de activos

CRITERIO	PUNTAJE	PONDERADOR	
Costo de reemplazo o reconstrucción	0 -5	30,00%	60%
Interrupción de servicios	0 -5	30,00%	
Requerimientos legales	0 -5	13,33%	40%
Imagen del Servicio	0 -5	13,33%	
Violación a la propiedad	0 -5	13,33%	

CATEGORÍA DE DOCUMENTO	DESCRIPCIÓN	RANGO
Secreto	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para el Gobierno Regional Metropolitano	4 - 5
Reservado**	Documentos que pueden producir impacto, pero pueden ser entregados sujetos a la normativa vigente	2 - 3
Pública	Pueden ser entregadas utilizando el canal de la Transparencia	0 - 1

Clasificación de los activos

Los funcionarios deben categorizar y tipificar los activos de los cuales es responsable.

**Categoría sólo para uso interno. Para efecto de la Ley corresponde a la categoría de tipo Pública

5.- Política de Dispositivos Móviles

Objetivo: Establecer los requisitos y controles para uso y conexión de equipos portátiles y dispositivos móviles.

Procedimientos:

- En el caso de pérdida, hurto, daño o deterioro del equipo, su reposición, reparación o mantenimiento es responsabilidad del funcionario. Así mismo, el funcionario deberá llenar el formulario "notificación pérdida dispositivo móvil" que se encuentra en la Intranet Institucional en un plazo no superior a 72 horas.
- El Servicio asigna servicio de Internet móvil a los funcionarios que salen frecuentemente a terreno. Los funcionarios deben acogerse a las Normas de uso Navegación por internet, las cuales prohíben, entre otros, la consulta de *páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los funcionarios*

5.- Política de Dispositivos Móviles

Rol del Depto. de Informática

- Establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios.
- Debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

5.- Política de Dispositivos Móviles

Rol del Depto. de Informática

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

5.- Política de Dispositivos Móviles

Rol del Depto. de Informática

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

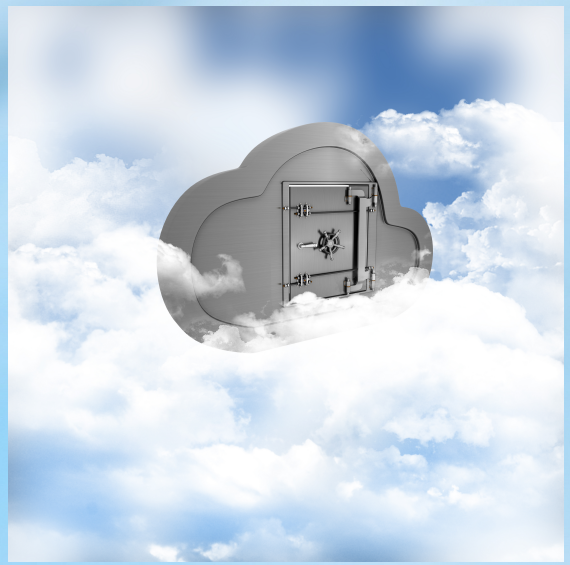
5.- Política de Dispositivos Móviles

Faltas a la Política

La seguridad de la información en todos sus ámbitos, debe ser considerada como un ítem dentro de la evaluación de desempeño del funcionario. El incumplimiento de las obligaciones y prohibiciones mencionadas en este documento y otros documentos complementarios, facultan al Gobierno Regional Metropolitano a aplicar medidas disciplinarias de acuerdo al Estatuto Administrativo.

6.- Procedimiento en Gestión de Claves

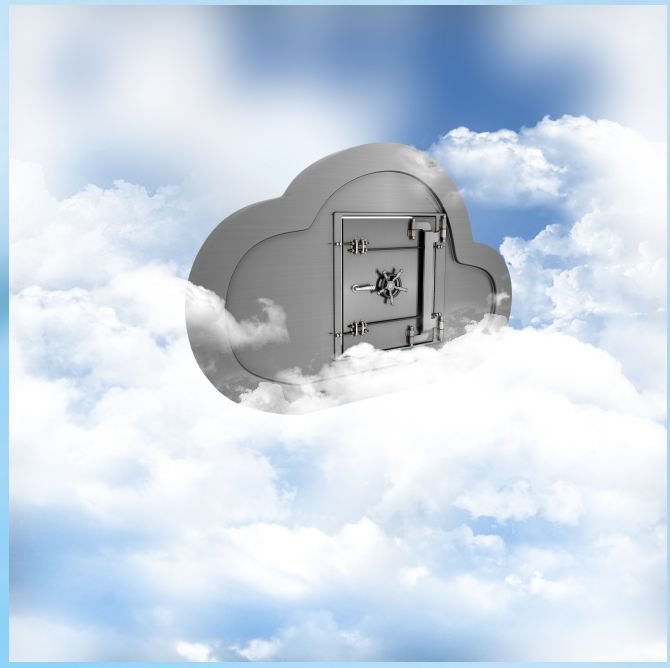
Objetivos: Establecer actividades necesarias para la gestión de derechos de acceso a los sistemas de información



Roles y responsabilidades

Jefatura de Unidad, Departamento o División.	• **Autorizar el Ingreso de Nuevos Funcionarios y notificar** • **Solicitar la creación o eliminación de los accesos a los sistemas de información.** • **Notificar cualquier desvinculación de funcionarios**
Funcionario designado del Departamento de Gestión de Personas.	• Solicitar los accesos a los sistemas de información. • Notificar cualquier desvinculación de funcionarios. • Recopilar y revisar los antecedentes mínimos para el inicio de tramites de ingreso y asignación de derechos de accesos provisorios.
Departamento de Informática	• Crear los accesos básicos a los nuevos funcionarios • Revisar y gestionar los permiso de accesos a los sistemas de información • Eliminar los derechos de accesos de los funcionarios que se desvinculan.
Encargado de Seguridad de la información	• Coordinar la Revisión de derechos de acceso de usuario.
Funcionarios	• Las responsabilidades de los funcionarios se describen en el punto 4.3

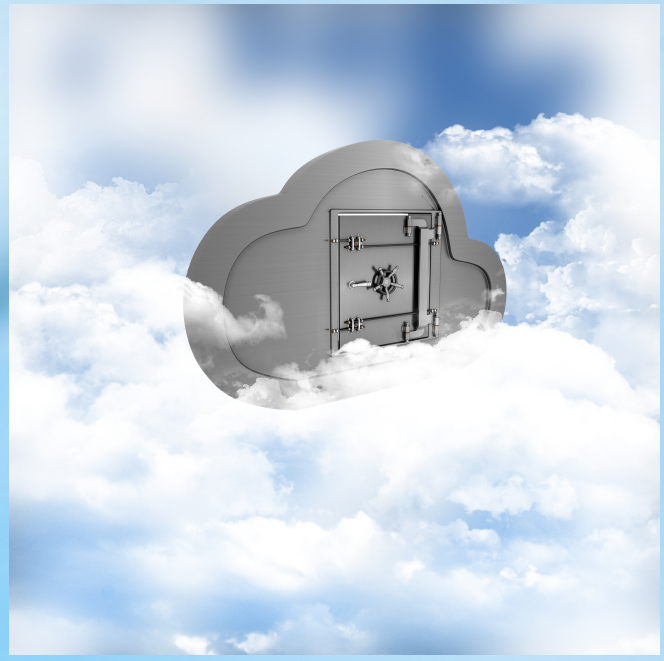
6.- Procedimiento en Gestión de Claves



Procedimiento: La Unidad de Soporte del Departamento de Informática es responsable de la creación de los accesos básicos de ingreso, que incluye:

- Creación de correo Electrónico.
- Creación de usuario en Active directory
- Creación de usuario en sistemas necesarios
- Habilitación de estación de trabajo

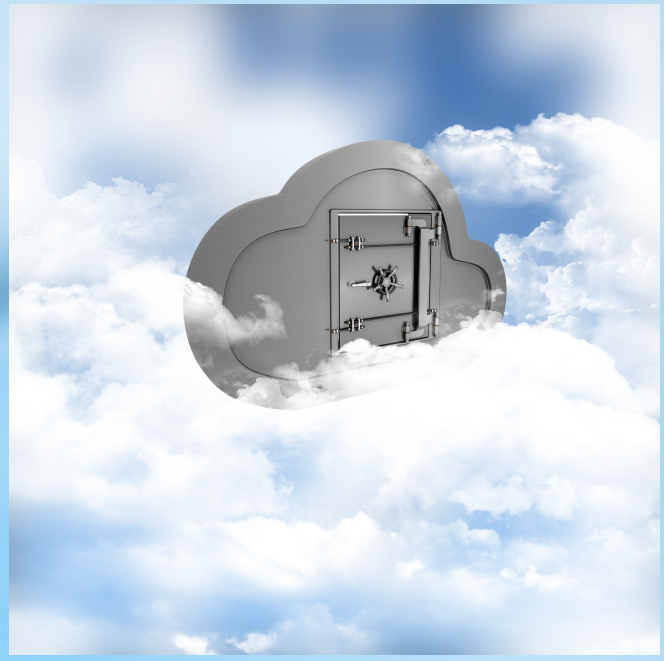
6.- Procedimiento en Gestión de Claves



Condiciones de uso:

- Mantener confidenciales las claves secretas.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en lodo lo que sea de su competencia.
- No divulgar información pertinente al Gobierno Regional Metropolitano.
- Entender la responsabilidad funcionaria , aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.
- La Jefatura de la Unidad, Departamento o División es responsable de solicitar la creación o eliminación de los accesos a los sistemas de Información mediante el Formulario de solicitud de creación/eliminación de accesos firmado.

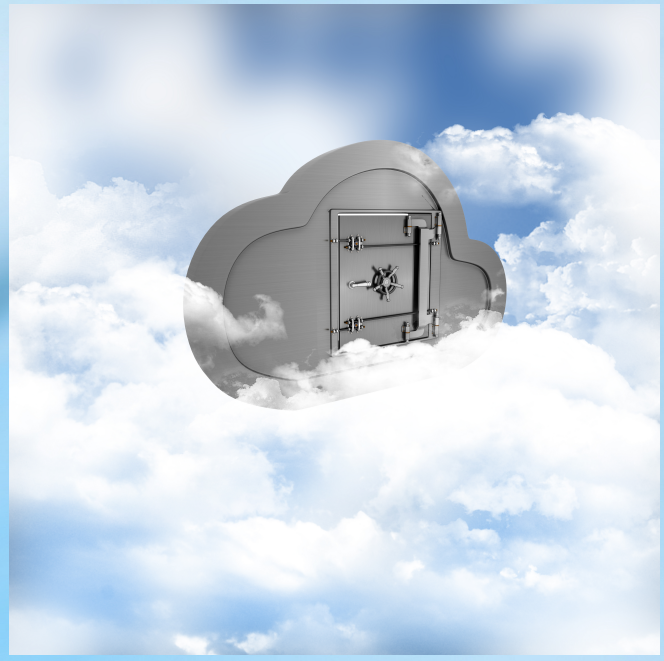
6.- Procedimiento en Gestión de Claves



Responsabilidades:

- Las contraseñas de acceso creadas por el usuario deben ser difíciles de adivinar.
- Los usuarios deben cambiar su contraseña de acceso con la frecuencia establecida por la Unidad de Soporte, como mínimo.
- Las contraseñas deben ser únicas para cada funcionario y deben cumplir, a lo menos, con los siguientes requisitos:
  - Debe contener 8 caracteres como mínimo.
  - No debe contener: los nombres o apellidos del funcionario, el user name o nombre de usuario, el nombre de la institución o unidad funcional.
  - No debe contener palabras completas.
  - Contener al menos un carácter de las siguientes categorías.

6.- Procedimiento en Gestión de Claves

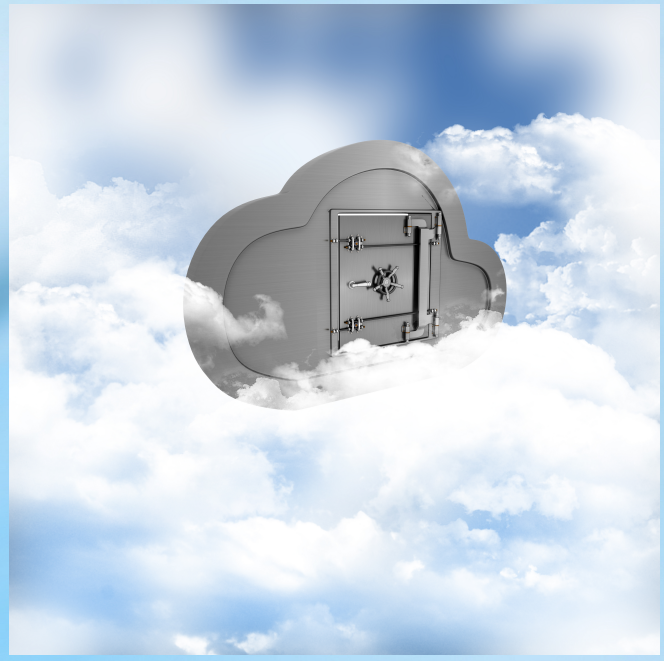


Ejemplo:

Categoría	Ejemplo
Letras Mayúsculas	A, B, C
Letras Minúsculas	A, b, c
Números	0,1,2,3,4,5,6,7,8,9
Símbolos	“, -, %, $, ¡, ¿…….

Ejemplo de Contraseña segura: **“J0Ab77c3**

6.- Procedimiento en Gestión de Claves



Intentos fallidos:

El número de intentos erróneos de acceso a una cuenta, debe estar limitado según se indique en el estándar definido por la Unidad de Soporte del Departamento de Informática.

7.- Política para la privacidad y protección de la información e identificación personal

Antecedentes: La protección de datos personales, esta garantiza en la ley 19.628 sobre la vida privada.

Objetivos: Garantizar el uso apropiado y la protección de los datos e información de carácter personal que pudieran almacenarse en las distintas plataformas, tanto informáticas, como en archivos físicos o digitales.

7.- Política para la privacidad y protección de la información e identificación personal

Definiciones

Dato Personal: cualquier información de personas naturales.

Dato Sensible: o a hechos o circunstancias de su vida privada o intimidad.

Seguridad de la Información: la prevención de la confidencialidad, integridad, disponibilidad de la información y la protección de la información.

Comunicación o transmisión de datos: dar a conocer de cualquier forma los datos de carácter personal.

7.- Política para la privacidad y protección de la información e identificación personal

Uso de Datos: cualquier operación o complejo de operaciones o procedimientos técnicos.

Almacenamiento de datos: la conservación o custodia de datos.

Documentos personales: se entenderá en esta política, documentos de carácter personal, que cada funcionario almacene en cualquier medio digital o físico.

Funcionarios: personas contratadas por el Servicio, indistintamente su calidad jurídica.

7.- Política para la privacidad y protección de la información e identificación personal

Responsabilidades.

Departamento de Informática: será el encargado de proveer de sistemas de seguridad de la información en las plataformas digitales de uso institucional.

Comité de Seguridad de la información: velará por impulsar medidas de seguridad de la información, difundir y capacitar en torno a las materias de protección de datos.

Funcionarios: todo funcionario es responsable de la información que almacena, administra y difunde, sea o no, relativa a sus funciones, propias o de terceros

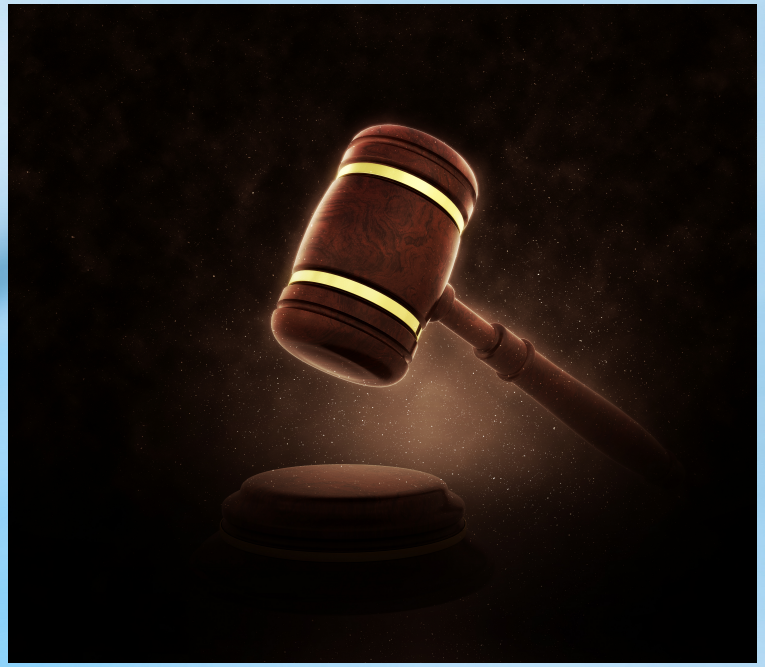
7.- Cumplimiento con las políticas y normas de seguridad

Objetivos: Las jefaturas deben revisar regularmente el cumplimiento de las políticas, normas y procedimientos de Información dentro de su Departamento.

Procedimiento

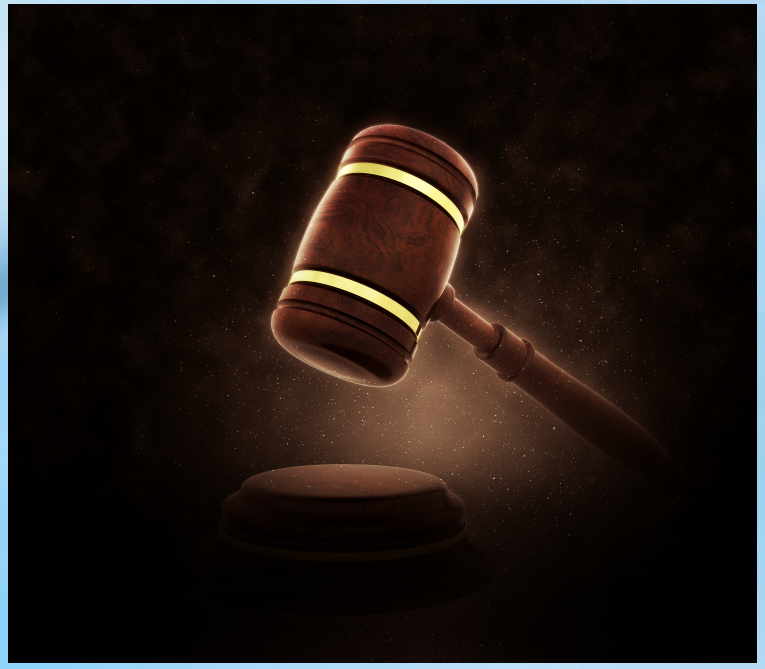
- Las Jefaturas deberían identificar cómo verificar que se cumplen los requisitos de seguridad de la Información definidos en las políticas, normas y otras normativas pertinentes.
- Los resultados de las revisiones y acciones correctivas que realizan los jefes de departamento se deben registrar y se deben mantener estos registros.
- Las jefaturas deben informar los resultados al Encargado de Seguridad cuando se realiza una revisión independiente en el área de su responsabilidad.

7.- Reglamento sobre infracciones al SSI



Objetivos: El presente Reglamento tiene por objeto establecer los principios y criterios que, de acuerdo con el sistema de seguridad de la información y los documentos asociados al mismo, permitan estimar que una conducta, mediante el uso de las tecnologías de información, pone en riesgo la confidencialidad, integridad y disponibilidad de información de relevancia para la institución.

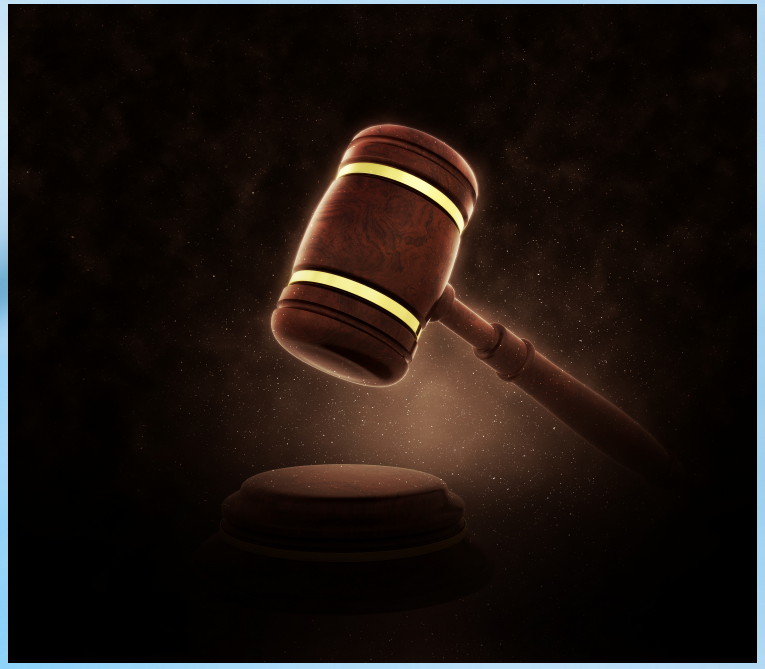
7.- Reglamento sobre infracciones al SSI



¿Que implica?

- Infracciones son los actos u omisiones que puedan poner en riesgo la confidencialidad, integridad, disponibilidad de la información, la continuidad operacional de los procesos institucionales y la entrega de productos y servicios.
- Quien tome conocimiento de un hecho que pudiere ser irregular tiene la obligación de ponerlo en conocimiento de su Jefatura directa y/o del Jefe Superior del Servicio.
- Cualquier violación de la seguridad de la información deberá ser informada de inmediato al Encargado de Seguridad.
- Podrá constituir una violación a la seguridad de la información no guardar secreto en los asuntos que revistan el carácter de reservados.

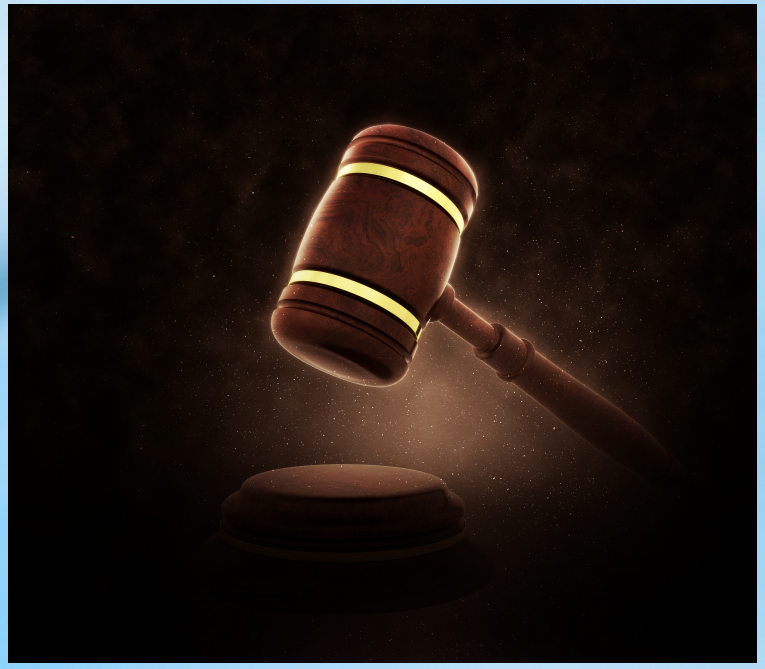
7.- Reglamento sobre infracciones al SSI



¿Que implica?

- Podrá considerarse una violación a la seguridad de la información el daño, sustracción o pérdida de información o documentos, en forma dolosa o negligente por parte de algún funcionario.
- En caso que una determinada situación o conducta pudiera ser constitutiva/o de infracción a las obligaciones o deberes funcionarios deberá ser puesto en conocimiento del Jefe Superior del Servicio.

7.- Reglamento sobre infracciones al SSI



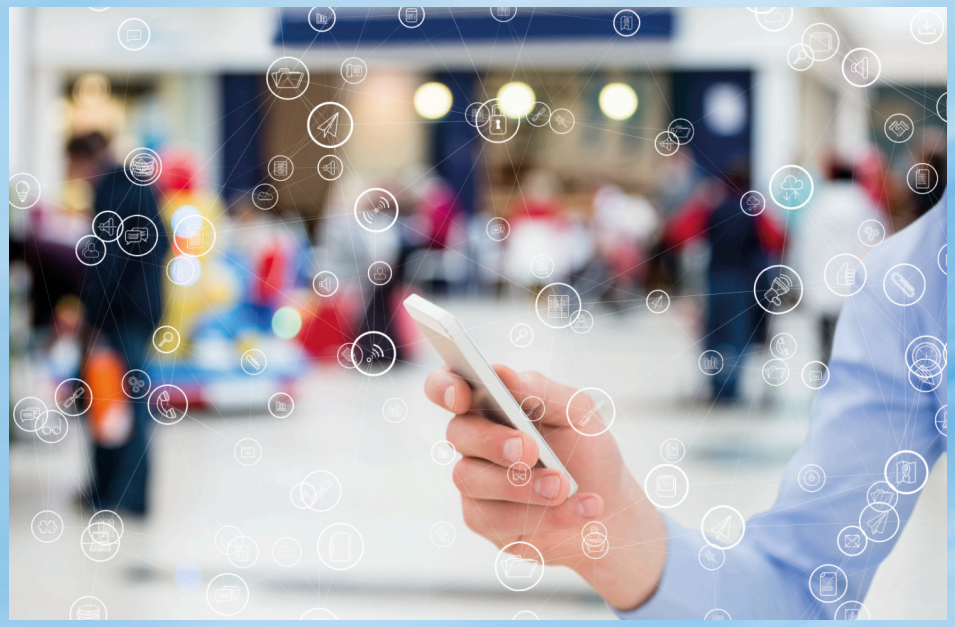
SANCION POSITIVA

El proceso disciplinario puede convertirse en una motivación o incentivo si se definen sanciones positivas para el comportamiento sobresaliente.

Es necesario destacar el buen uso en el Sistema de seguridad de la información e incentivar a los funcionarios a poder denunciar faltas a la seguridad.

8.- Recordar

- Mantén tu escritorio limpio, sin claves anotadas en tacos o papeles.
- Deja tu PC bloqueado si no estas.
- Cambia tu contraseña constantemente.
- No compartas tu contraseña.



8.- Recordar

- Si vas a terreno no conectes tu dispositivo móvil a WIFI publicas.
- Mantén tu dispositivo con clave.
- No descargues aplicaciones en Dispositivos Móviles institucionales
- Informa inmediatamente en caso de perdida