A5_1_1Política de Seguridad

Clasificación de la Información:

Nivel del Documento	Documentos del SGSI
Nombre del Fichero	A5_1_1PoliticadeSeguridad-V2.0.docx
Tipo	RESTRINGIDO
Ámbito de Difusión	Todos los empleados y colaboradores externos de INSTITUTO INTER
Responsable	Responsable de Seguridad de INSTITUTO INTER Director General de INSTITUTO INTER

CONTROL DE MODIFICACIONES		
Descripción	**Versión**	**Fecha**
Se actualizan los roles y responsabilidades, así como las leyes, ya que algunas se han derogado como la Ley Orgánica 15/1999 de 13 de diciembre	2.0	28/12/20

ELABORADO:	REVISADO:	APROBADO:
Jose Ivorra	**Jose Ivorra**	**Dirección General**
Fecha: 02/01/2017	**Fecha:** 28/12/2020	**Fecha:**
Firma (opcional):	**Firma (opcional):**	**Firma (opcional):**

ÍNDICE DE CONTENIDO

1. POLÍTICA DE SEGURIDAD

Para nuestra organización es de vital importancia la confianza generada por nuestros alumnos que acceden a la modalidad de formación para el empleo (SERVEF). En este proceso, nos confían información, la cual tenemos que gestionar y tratar por mediación de nuestros Sistemas de Información con totales garantías de seguridad. La Política de Seguridad tiene como misión establecer objetivos de Seguridad y proteger los activos de información a todos los niveles, y se desarrolla en base al objetivo de mejora continua aprobado por la dirección y especificado en el SGSI01 “Alcance del SGSI”

Estos objetivos incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento con la finalidad de proteger la información otorgada por los alumnos de INSTITUTO INTER. Asimismo, se detallan las precauciones y medidas de seguridad adoptadas para asegurar el correcto cumplimiento de la legislación vigente: “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD), “Ley de Medidas de Impulso de la Sociedad de la Información”, Ley 56/2007.

Queda también regulada la cesión de información a terceras personas, quedando estrictamente prohibida la cesión de información sensible de la Organización fuera de los procedimientos establecidos, siendo necesaria la autorización de la Gerencia para cualquier salida de información fuera de INSTITUTO INTER.

Esto es extensible para cualquier cesión de información que se realice a terceras entidades. Solo se permite dicha cesión cuando esté regulada por un acuerdo entre ambas partes para el intercambio de dicha información y en el mismo se defina la finalidad exacta de dicha cesión, así como la caducidad de la misma y la garantía de supresión de la misma una vez cumplido el objetivo de la cesión.

El objetivo principal de la creación de esta política de Seguridad por parte del Responsable de Seguridad y de la Dirección General de INSTITUTO INTER es garantizar a los usuarios el acceso a la información con la cantidad y calidad que

se requiere para el desempeño del trabajo, así como evitar pérdidas de información y accesos no autorizados a la misma.

Esta política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos estratégica de la organización. A este efecto y para gestionar los riesgos que afronta INSTITUTO INTER se define un procedimiento de evaluación de riesgos definida en proceso de gestión de riesgos del SGSI.

De igual forma se establecen los siguientes principios que deben respetarse:

Confidencialidad: La información gestionada por INSTITUTO INTER, debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

Integridad: La información de INSTITUTO INTER, debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.

Disponibilidad: La información de la organización está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

2. ENTORNO DE GESTIÓN DE LA SEGURIDAD

La organización dispone de un Sistema de Gestión de Seguridad de la Información. Todas las políticas y procedimientos incluidos en este documento y en el Sistema han sido revisados, aprobados e impulsados por la Dirección General de INSTITUTO INTER

1.1. ALCANCE

Empleados

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que se encuentren afectados por el alcance del SGSI y especialmente del Departamento de Sistemas de la organización para su aseguramiento. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad de la Información y su documentación asociada. Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad, durante la duración de su contrato o tras la extinción del mismo, estarán sujetos a acciones disciplinarias según se contempla en el punto seis (6) de este documento.

Los sistemas

Esta Política afecta a todos los activos de Información de la organización implicados en el alcance del SGSI cualquiera que sea su naturaleza y soporte (automatizado o no), tanto a la documentación en formato papel, como a los PCs personales o servidores, redes, aplicaciones, Sistemas Operativos, procesos de la organización que pertenecen y/o son administrados por INSTITUTO INTER Esta política cubre los aspectos directamente más relacionados con la responsabilidad y buen uso del personal.

1.2. ROLES Y RESPONSABILIDAD

El Responsable de Seguridad de la Información es el responsable de establecer y mantener las Políticas de Seguridad de la Información, estándares, directivas y procedimientos de la Organización.

El procedimiento de Auditorías Internas asegura el alineamiento de las Tecnologías de la Información con las Políticas, Procedimientos y Legislación Aplicable.

Las Incidencias relacionadas con la Seguridad de los Sistemas de Información y los incumplimientos de la Política de Seguridad serán comunicadas al Departamento de Sistemas, y gestionadas por el Responsable de Seguridad de

la Información.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad de la Información son atribución de la Dirección General de INSTITUTO INTER y de los órganos de gobierno según la legislación aplicable.

1.3. CATEGORIA DE RESPONSABILIDADES

Con tal de coordinar los esfuerzos de Seguridad, la organización divide las responsabilidades del personal en tres categorías:

Responsabilidades del usuario

Los usuarios deben conocer y aplicar las políticas de Seguridad de la Información, procedimientos, estándares y aplicar la legislación vigente. Deben entenderlos perfectamente y cumplir con los mismos.

Responsabilidades del propietario

Los propietarios de Activos de Información generalmente se corresponden con la Gerencia, o responsables de Área, quienes deben adquirir, desarrollar y mantener aplicativos de la organización como sistemas de soporte a las decisiones y otras actividades de la misma.

Los propietarios deben indicar la clasificación de sus activos que mejor corresponde con su valor crítico, disponibilidad e importancia relativa para la organización.

Su clasificación marcará el nivel de riesgo y de protección, así como el nivel de acceso a dicha información o aplicativo.

Administradores de Información

Los administradores son empleados a cargo de salvaguardar la Información de la Organización propia y cedida por terceros.

El Responsable de Seguridad y el Departamento de Sistemas mantienen información de los PCs y dispositivos personales y actúan como administradores en algunos de ellos.

Cada Sistema de Información debe disponer al menos de un Administrador autorizado según consta en el Inventario de Activos. Son los responsables de Almacenar la Información, implementar controles de acceso (para prevenir acceso no autorizados) y ejecutar copias de Seguridad periódicas (para asegurar la disponibilidad de la información crítica).

Los administradores deben asimismo desarrollar, aplicar, mantener y revisar las medidas de Seguridad definidas por los propietarios de la Información.

3. CLASIFICACIÓN DE LA INFORMACIÓN

Responsabilidad de la confidencialidad de la información

Cada uno de los empleados es responsable de prevenir la salida de información no autorizada. En particular la persona que produce la información es responsable de clasificarla y asegurar su custodia.

El responsable de cada área está encargado de que se respete la confidencialidad de información dentro su grupo.

Clasificación de la información conforme a su sensibilidad

La información de INSTITUTO INTER está clasificada en 3 categorías dependiendo de su grado de confidencialidad. Todo empleado debe ser consciente de esta clasificación:

1. **NO CLASIFICADA** (PUBLICA): Esta información puede ser compartida sin restricciones. Como ejemplo, notificaciones del tablón de anuncios o emails sobre temas sin importancia.
2. **RESTRINGIDA** (USO INTERNO Y DE DIFUSION LIMITADA): La información Restringida de uso interno (datos de cursos, alumnos,

profesores) puede ser compartida libremente entre los empleados contratados y subcontratados que hayan firmado acuerdo de confidencialidad según su perfil de acceso, y la información restringida de difusión limitada puede ser compartida entre las partes interesadas (clientes, proveedores, etc.) con algún tipo de contrato, oferta, descripción de proyecto, etc. Por ejemplo, los datos de alumnos, cursos y profesores para terceras entidades que lo soliciten, o el acceso restringido de los profesores a los datos de los cursos que ellos gestionan, pero no al resto de documentación de cursos

3. .

4. **CONFIDENCIAL**: Esta información debe ser únicamente compartida entre personal seleccionado que necesite ser conocedor de la misma. Ejemplos son;

    - Información clasificada (planes de formación, memorias de acciones formativas, etc.)
    - Información confidencial referente al personal
    - Datos de carácter personal (datos personales de nivel medio y alto de alumnos y profesores, incluyendo datos de salud). Esta información se rige por el Reglamento de Medidas de Seguridad vigente.

Etiquetado de la Información

La persona que produce la información decide sobre su clasificación, en función de lo expuesto en el punto anterior. Esta persona es también responsable de su reclasificación en etapas posteriores.

Reglas para manejo y custodia

NO CLASIFICADA (PUBLICA)

La persona que produce la información en este caso debe aprobar su difusión exterior, pudiendo incluir su aparición en Internet.

RESTRINGIDA

La información puede estar compartida entre los empleados de INSTITUTO INTER en función de sus necesidades de acceso.

La información Restringida se almacena físicamente en los servidores de INSTITUTO INTER, y es accesible únicamente a través de las Aplicaciones de Gestión y/o a través de la red corporativa, con un control de accesos.

Cualquier información accesible a través de la red y a través de las "Aplicaciones de Gestión Interna" se considera información restringida.

Cuando un empleado genere, reciba o clasifique información restringida, debe almacenarla con el control de accesos adecuado.

En caso de que la información restringida deba ser accesible sin conexión a los sistemas de la organización, se permitirá una copia de la misma en la máquina local o en un medio de almacenamiento extraíble, dentro de una carpeta con acceso exclusivo al usuario que deba utilizarla, y procediendo al borrado seguro de la información una vez deje de ser necesaria.

La mayoría de esta documentación es de uso interno y no debe ser propagada a través de ningún medio ni salir de la organización a través de ningún soporte.

La información de uso restringido que se intercambia con determinados clientes o proveedores (ofertas, contratos…) debe realizarse a través de medios seguros y fiables y con una clara referencia a la distribución exclusiva del documento entre las personas autorizadas.

Cualquier pérdida de información sensible o uso no autorizado debe ser comunicada inmediatamente al propietario de la información y al Responsable de Seguridad.

CONFIDENCIAL

Debe figurar la referencia ***"Confidencial"*** en la portada y a lo largo de cualquier documento clasificado como confidencial.

La información confidencial debe almacenarse con las medidas de control de acceso limitado al personal autorizado. Existe información confidencial accesible

a través de “Aplicaciones de Gestión”, las cuales deben incluir todas las medidas de Seguridad exigidas en este documento, entre ellas:

1. No distribuir más copias de las estrictamente necesarias.
2. Archivar en red o en local con control de accesos en caso de documentos confidenciales, de forma que solo permita el acceso al personal autorizado.
3. Si la información es archivada en formato papel, deberá custodiarse bajo llave.
4. Cuando la información confidencial, se envíe a través de redes públicas, la comunicación se realizará cifrada, para ello se cifrarán los documentos usando herramientas de compresión de archivo que permitan su cifrado (Como RAR con AES-128 o ZIP con AES-256), comunicándose la clave al receptor preferentemente por vía telefónica o en su defecto en otro correo. Las claves serán de un solo uso.
5. No publicarla en la web.
6. Cuando se saca la información fuera de INSTITUTO INTER:
    - Debe tenerse el permiso expreso y por escrito del Jefe de Servicio.
    - La información debe viajar cifrada.
    - No se dejará la información desatendida en ningún momento.
    - Se tomarán medidas de protección para evitar su robo.

La destrucción de cualquier documento escrito confidencial debe realizarse de manera segura en las destructoras de papel disponibles, análogamente cualquier soporte extraíble con información confidencial deberá ser destruido o formateado de manera segura según los procedimientos establecidos.

DATOS DE CARÁCTER PERSONAL

Dentro de los datos confidenciales, los datos de carácter personal están identificados en el Documento de Seguridad relativo a la LOPD de INSTITUTO INTER, donde constan todos los ficheros clasificados y los controles y personal autorizado para su uso.

Los datos de carácter personal temporales cedidos por terceros deben mantener las medidas de Seguridad correspondientes y deben estar almacenados como información confidencial.

En las auditorías periódicas de SGSI se comprobará el cumplimiento de estas políticas por parte de los usuarios.

4. POLÍTICAS DE SEGURIDAD DEL PERSONAL

Se han diseñado unas políticas que deben ser llevadas a cabo a la hora de acceder a la información de la Organización y que responden a la siguiente clasificación:

4.1.- Del equipo de trabajo

De la instalación del equipo informático

1. Todo el equipo informático (PCs, servidores, teléfonos móviles, ordenadores de bolsillo, otros dispositivos...), que corresponda al uso exclusivo de personal contratado por INSTITUTO INTER está sujeto a las normas y procedimientos de instalación que emite el Departamento de Sistemas bajo supervisión del Responsable de Seguridad de la Organización o el personal designado por éste. La instalación de cualquier programa deberá disponer de autorización por su parte.
2. El equipo de la Organización que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en el CPD (Centro de Proceso de Datos) habilitado a tal efecto, las condiciones ambientales, la alimentación eléctrica y su acceso está regulado mediante los mecanismos oportunos.
3. Los usuarios de los equipos de uso personal deberán responsabilizarse de cumplir con las políticas de seguridad establecidas por INSTITUTO INTER

4. Los responsables de las distintas áreas de los departamentos con personal y acceso a la información de la Organización deberán en conjunción con el Responsable de Seguridad dar cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, adjudicación, etc., tanto del personal como de los equipos de uso exclusivo del mismo.
5. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, al Responsable de Seguridad.

Del mantenimiento del equipo informático

1. Cada equipo destinado en exclusiva al trabajo para la Organización, aun perteneciendo a una entidad externa, será responsabilidad de la persona a que haya sido asignado.
2. Cualquier cambio en el puesto de trabajo y/o de cualquier PC y material de la organización deberá ser registrado.
3. El acceso desde ordenadores portátiles y otros dispositivos móviles a la información de la Organización (para consultorías externas, asesorías, trabajo de personal con movilidad...) se hará solicitando el mismo al Responsable de Seguridad, el cual otorgará un acceso temporal a los recursos necesarios de la Organización con la finalidad con que se disponga, comprometiéndose el usuario de dicho dispositivo a no mantener ninguna copia en local de dicha información y cumplir con los normas establecidas para el acceso a la misma expuestas en este documento.

4.2.- Del control de accesos

Del acceso a áreas críticas.

1. El acceso de personal se llevará a cabo de acuerdo a las normas y procedimientos establecidos por INSTITUTO INTER

2. El acceso al CPD está restringido al personal del Departamento de Sistemas, y en todo caso, las visitas externas se realizan siempre escoltadas por un empleado del Departamento.
3. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las instalaciones estará sujeto a las que especifique gerencia o los servicios de Seguridad si peligra la integridad de los bienes o las personas.

Del control de acceso al equipo informático

1. Todos y cada uno de los equipos son asignados a uno o más usuarios, por lo que es de su competencia hacer buen uso de los mismos.
2. Cada trabajador se encargará de llevar a cabo las siguientes prácticas de Seguridad recomendadas en su equipo:
    - Iniciar sesión como usuario de la organización y regirse por las normas en cuanto a política de contraseñas de la organización.
    - Cerrar la sesión fuera del horario de trabajo, así como evitar el uso de la misma por terceras personas.
    - Proteger el escritorio del mismo durante las ausencias del puesto de trabajo en horario de oficina, mediante el bloqueo del PC. Los equipos se configuran con protección por contraseña que se activa tras un período de inactividad. En equipo multiusuario, se configurará el equipo para el cierre de sesión automático dado un período considerado de inactividad igualmente.
    - Guardar las contraseñas en lugar seguro, y no revelar las contraseñas personales a nadie.
    - Disponer de la cuenta de correo facilitada por la organización y emplear dicha cuenta para cualquier comunicación interna o externa.
    - Emplear el correo de una manera responsable, y no emplear recursos productivos facilitados por INSTITUTO INTER para usos no pertinentes.

- Comunicar cualquier incidencia de Seguridad (posible virus, comportamientos sospechosos...) al Departamento de Sistemas.

3. El acceso a información corporativa se realizará a través de la red de datos corporativa.
4. El acceso a datos corporativos también se realizará mediante la Intranet, cuyo acceso estará limitado a los usuarios que deban usarla mediante autenticación por nombre de usuario y contraseña.

Política de contraseñas

1. Todos los empleados que necesitan acceso a algún Sistema de Información de la organización disponen de un Identificador ID de usuario único y una contraseña personal.
2. El usuario asociado a cada empleado está conforme a los privilegios que corresponden a sus funciones, responsabilidades y actividades.
3. Todos los usuarios son responsables de proteger sus identificadores de usuario y contraseñas.
4. Las contraseñas escogidas por los usuarios deben ser difíciles de adivinar y no deben contener información relacionada con su trabajo y su vida personal: Números de teléfono, nombre de familiares, direcciones, números personales (PIN, SIN, DNI…), lugares conocidos, etc…
5. Las contraseñas deben ser cambiadas con la periodicidad y cumplir las normas establecidas para cada sistema.
6. Las contraseñas no deben ser almacenadas en ficheros legibles, macros, PCs sin control de acceso o ningún otro lugar donde puedan ser accedidas por personas sin autorización.
7. Los administradores del sistema y personal técnico nunca solicitarán la contraseña a sus usuarios. La única excepción es la asignación inicial de la

contraseña con el compromiso por parte del usuario de cambiarla en cuanto acceda al sistema.

8. Si un usuario sospecha que su identificador y contraseña está siendo utilizado ilegalmente, es su responsabilidad avisar inmediatamente a los Administradores del Sistema.

De control soporte en papel.

Es responsabilidad de todo empleado no dejar abandonada información confidencial en la impresora, fax o dispositivos similares, así como dejarla desatendida en el puesto de trabajo.

De control de acceso remoto.

La organización no dispone de una conexión remota a su red para usuarios fuera de su puesto de trabajo. En el caso de que se habilitara, los permisos serán los mismos que desde su puesto de trabajo local, y la conexión remota se realizará de forma cifrada y mediante el uso de dispositivos criptográficos para autenticarse.

El potencial usuario remoto se compromete a adoptar las medidas de Seguridad en su equipo para garantizar que el acceso a los datos se realiza de manera responsable.

El usuario de estos servicios deberá sujetarse a lo expuesto anteriormente sobre acceso local al equipo.

Del Acceso a Internet.

Los accesos a Internet a través de los navegadores deben sujetarse a las normas éticas y es responsabilidad de cada usuario realizar un uso lícito de los medios de que le provee la organización para el correcto desempeño de su trabajo.

El acceso Web a la Intranet de la Organización se realizará desde cualquier puesto de trabajo, y es protegido mediante el control de accesos.

Toda la programación involucrada en la tecnología Web deberá cumplir unos requisitos de calidad y de seguridad.

El material que aparezca en la página web deberá ser aprobado por la Dirección General de INSTITUTO INTER, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

Está prohibido representar a la organización en foros, listas de correos, etc… sin la autorización expresa de la Gerencia.

4.3.- De utilización de los recursos de la red

1. Todos los empleados que utilicen los Sistemas de Información de la Organización deben firmar la aceptación de esta Política de Seguridad. Al firmar esta política, el empleado acepta comprender y comprometerse al cumplimiento de las políticas y procedimientos de la organización relativas al uso de los Sistemas de Información, incluyendo las normas de la presente política.
2. El uso del correo electrónico para comunicaciones corporativas estará limitado a las cuentas de la organización, y deberá cumplir con el propósito del desempeño del trabajador, siendo necesaria la inclusión en los mensajes de correo salientes de la cláusula relativa a la confidencialidad de los datos y la utilización del contacto de correo electrónico exclusivamente para el fin de dicho correo.
3. La cesión de datos a través de este medio deberá estar autorizada para la finalidad exclusiva para la cual sea necesario. Está prohibido copiar, sin justificación o autorización, información propia de la organización o software. Aquellos responsables de reenvío de información a terceros sin autorización estarán sujetos a la aplicación de medidas disciplinarias. Incluido en este apartado está la prohibición de enviar cartas o solicitudes así como transmitir cualquier software no validado por la organización.
4. Se hará un uso responsable de otras cuentas personales para uso particular en la organización.

5. Será responsabilidad del usuario la apertura de mensajes de correo. Se aconseja no abrir correos electrónicos no solicitados, de remitentes desconocidos o de remitentes conocidos de los que no se espera ningún correo electrónico. Es responsabilidad igualmente del usuario el buen uso del correo electrónico, si bien se dispondrán las medidas técnicas por parte de INSTITUTO INTER para evitar el spam de correo, las cuentas no autorizadas, etc. Debido a que las cuentas de correo electrónico corporativas son cedidas por la organización para uso profesional del empleado, el usuario deberá atenerse a las reglas establecidas para su uso por la organización.

4.4.- De utilización de Soporte de Información

Se prohíbe expresamente la salida de soportes de información extraíble (dispositivos de almacenamiento USB, memorias flash, etc.) con datos confidenciales o restringidos de INSTITUTO INTER, sin el consentimiento expreso del Responsable de Seguridad. Cuando se usen dichos dispositivos dentro de INSTITUTO INTER los usuarios deben ser conscientes de ejecutarlos solo en equipos con antivirus actualizados y conocer perfectamente el origen de dicho medio y que sea confiable.

Cualquier información que sea almacenada en un soporte de información extraíble deberá ser empleada exclusivamente para motivos de trabajo, y la información deberá eliminarse o guardarse bajo llave una vez deje de ser útil.

4.5.- De supervisión y evaluación

1. La organización se reserva el derecho de monitorizar e inspeccionar el correcto uso de los Sistemas de Información por parte de los empleados en cualquier momento, respetando la legislación vigente en cuanto al derecho de privacidad de los empleados. Estas comprobaciones puede llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado, y se llevarán a cabo con el consentimiento expreso del responsable de la Gerencia.

2. Periódicamente se realizará un escaneo en la red empleada por la INSTITUTO INTER en busca de posibles fallos y vulnerabilidades, así como de virus en los PCs, servidores y recursos de la Organización, y una actualización del inventario de aplicaciones y uso de los recursos de cada PC.
3. Con una periodicidad **mínima anual** se revisará esta Política de Seguridad para adecuarla a los cambios en la Organización, y se registrarán las incidencias y no conformidades encontradas en el sistema, elaborando una lista de acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad y el buen uso de los recursos de la Organización.
4. Los sistemas considerados críticos, están bajo monitorización permanente.
5. Se realizarán las copias de Seguridad y recuperación de ficheros según las normas establecidas en los procedimientos correspondientes.
6. Cualquier incidencia acaecida en los sistemas de información será registrada y se gestionará según las normas establecidas en los procedimientos correspondientes. Las incidencias que afecten a la LOPD, serán marcadas como tales.
7. Periódicamente se llevará a cabo por parte de una tercera organización la auditoría de cumplimiento de la LOPD (“Ley Orgánica de Protección de Datos”), así como auditorías del Sistema de Gestión de la Seguridad de la Información (SGSI).

4.6.- Propiedad Intelectual del material Desarrollado en la organización

1. INSTITUTO INTER tiene derechos exclusivos sobre patentes, copyrights, licencias, desarrollos y cualquier otra propiedad intelectual desarrollada por sus empleados con motivo de su trabajo en INSTITUTO INTER

2. Todos los desarrollos y documentos producidos o provistos por los empleados para el propósito de la organización son propiedad de INSTITUTO

INTER y se reserva el derecho de acceso y utilización de esta documentación en virtud de los intereses de la organización.

5. GENERALES

1. El departamento de sistemas deberá de emitir los planes de contingencia que correspondan a las actividades críticas que realicen.
2. Debido al carácter confidencial de la información, el Responsable de Seguridad deberá actuar de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

6. SANCIONES

1. Cualquier violación de las políticas y normas de seguridad será sancionada de acuerdo a los mecanismos habilitados en la legislación vigente.
2. Todas las acciones en las que se comprometa la seguridad de INSTITUTO INTER y que no estén previstas en esta política, deberán ser revisadas por Gerencia y por el Responsable de Seguridad para dictar una resolución sujetándose al criterio de la organización y la legislación prevista.

Notas

1. Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la plantilla de personal, cambio en la infraestructura, desarrollo de nuevos servicios, entre otros.

2. Esta política de seguridad debe ser difundida a todo el personal involucrado en la relación con la Organización que maneje datos y recursos pertenecientes a la misma.

7. DOCUMENTOS RELACIONADOS

- Memorándum a los empleados (SGSI04)
- Manual de Seguridad (SGSI05)
- Compromiso de Aceptación de la Política de Seguridad por parte de los empleados (SGSI06)
- Procedimiento de Gestión de la Documentación (PR01)

8. REGISTROS

- Archivo de todas las aceptaciones por parte de todos los usuarios internos o externos del documento ***"Compromiso de Aceptación de la Política de Seguridad por parte de los empleados"*** (***SGSI06***).
- Documento de ***"Aprobación por parte de la Dirección General de la Política de Seguridad de la Información"*** (***F0001***).

9. APROBACIÓN

La presente Política de Seguridad ha sido aprobada por la Gerencia, con vigencia a partir de la fecha de su firma.