GOBIERNO REGIONAL
HUANCAVELICA

Resolución Gerencial General Regional

Nro. 348 -2020/GOB.REG-HVCA/GGR

Huancavelica, 22 SEP 2020

VISTO: El Informe N° 199-2020/GOB.REG.HVCA/GGR-ORAJ con Reg. Doc. N° 1606303 y Reg. Exp. N° 1185205, el Informe N° 145-2020/GOB.REG.HVCA/GGR-GRPPyAT, el Informe N° 131-2020/GOB.REG.HVCA/GRPPyAT-SGDIyTI, el Oficio Múltiple N° D000029-2020-PCM-SEGDI; y,

CONSIDERANDO:

Que, de conformidad con el artículo 191 de la Constitución Política del Estado, modificado por Ley N° 27680 – Ley de Reforma Constitucional, del Capítulo XIV, del Título IV, sobre Descentralización, concordante con el artículo 31 de la Ley N° 27783 – Ley de Bases de la Descentralización, el artículo 2 de la Ley N° 27867 – Ley Orgánica de Gobiernos Regionales y el artículo único de la Ley N° 30305, los Gobiernos Regionales son personas jurídicas que gozan de autonomía política, económica y administrativa en los asuntos de su competencia;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo N° 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia N° 4, la implementación de mecanismos para mejorar la seguridad de la información, siendo necesario contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en las infraestructuras críticas, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, mediante Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014-CNB-INDECOPI, se aprueba la NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición; Norma Técnica Peruana que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Asimismo, incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización;

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

Que, en este contexto normativo, el Sub Gerente de Desarrollo Institucional y Tecnologías de la Información mediante Informe N° 131-2020/GOB.REG.HVCA/ GRPPyAT-SGDIyTI, presenta el Manual de Seguridad de la Información del Gobierno Regional de Huancavelica que tiene como objetivo definir claramente el propósito de implementación de gestión de seguridad de los sistemas informáticos, redes, servidores y usuarios finales;

Que, estando a lo expuesto, corresponde aprobar el Manual de Seguridad de la Información del Gobierno Regional de Huancavelica, que será de aplicación en todas las actividades realizadas en la implementación del Sistema de Gestión de Seguridad de la Información de nuestra Entidad Regional;

Estando a lo informado; y,

Con la visación de la Gerencia Regional de Planeamiento, Presupuesto y

GOBIERNO REGIONAL
HUANCAVELICA

Resolución Gerencial General Regional

Nro. 344 -2020/GOB.REG-HVCA/GGR

Huancavelica, 22 SEP 2020

Acondicionamiento Territorial, Oficina Regional de Asesoría Jurídica y la Secretaría General;

En uso de las atribuciones conferidas por el numeral 6 del artículo 28 del Reglamento de Organización y Funciones del Gobierno Regional aprobado por Ordenanza Regional N° 421-GOB.REG.HVCA/CR y la Resolución Ejecutiva Regional N° 107-2020/GOB.REG.HVCA/GR;

SE RESUELVE:

ARTÍCULO 1°.- APROBAR el **Manual de Seguridad de la Información del Gobierno Regional de Huancavelica**, que en calidad de anexo forma parte integrante de la presente Resolución.

ARTÍCULO 2°.- NOTIFICAR, la presente Resolución a los órganos competentes del Gobierno Regional de Huancavelica y la Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información, para los fines pertinentes y su publicación en el portal institucional.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

GOBIERNO REGIONAL
HUANCAVELICA
Ing. Ciro Soldevilla Huayllani
GERENTE GENERAL REGIONAL

GOBIERNO REGIONAL DE HUANCAVELICA
V° B°
Ing Roncisco Arana Huamán
JEFATURA REGIONAL DE PLANEAMIENTO, PRESUPUESTO Y ACONDICIONAMIENTO TERRITORIAL

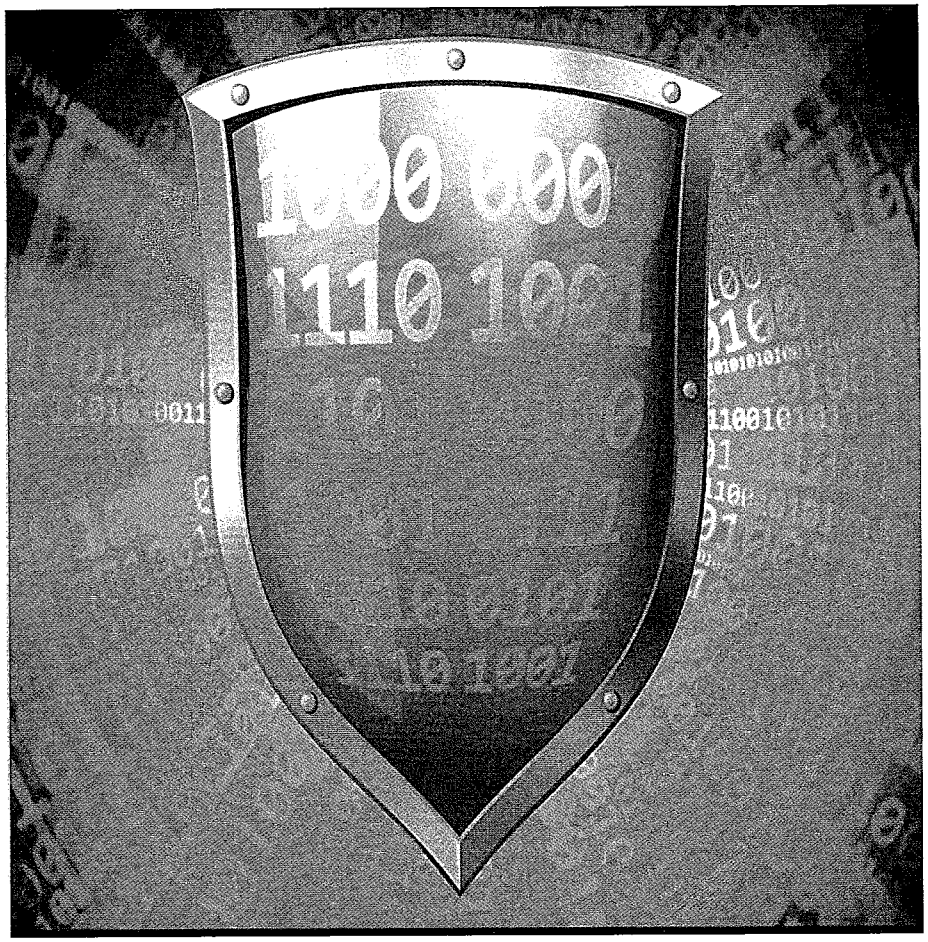
GOBIERNO REGIONAL DE HVCA
V°B°
Abog. Hector J. Riveros Carhuapoma
DIR. REG. DE ASESORÍA JURÍDICA

GOBIERNO REGIONAL HVCA
V°B°
Abog. Ciro Dennis Torres Rodríguez
Secretario General

CDTR/cgme

Gobierno Regional
HUANCAVELICA

MANUAL DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE HUANCAVELICA



GOBIERNO REGIONAL
Gerencia de Desarrollo Institucional y Tecnologías de la Información
V° B°
Ing. Cesar J. Altamirano Flores
HUANCAVELICA

SUB GERENCIA DE DESARROLLO INSTITUCIONAL Y TECNOLOGIAS DE INFORMACIÓN

AGOSTO 2020

Gobierno Regional
HUANCAVELICA

GENERALIDADES

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las instituciones públicas privadas deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya que les permite mantener una ventaja competitiva frente a otras empresas [NTP ISO/IEC 17799].

La seguridad de la información se encarga de la búsqueda de la preservación de la confidencialidad, integridad y disponibilidad de la información [NTP ISO/IEC 17799], es decir, buscar proteger tanto de ataques físicos, tales como robos o incendios, como de ataques cibernéticos, tales como el aprovechar vulnerabilidades de los sistemas de información.

En nuestro país, desde hace más de diez años, las políticas del gobierno han ido recomendando una adecuada gestión de la seguridad de la información con resoluciones ministeriales tales como la N° 224-2004-PCM en la que aprueban el uso obligatorio de la NTP ISO/IEC 17799:2004 en las entidades públicas referente a las buenas prácticas para gestionar la seguridad de la información [NTP ISO/IEC 17799].

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V°B° Ing. César J. Andaluano Flores HUANCAVELICA

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la norma técnica peruana (NTP) – ISO/IEC 27001:2014 mediante la resolución N° 129-2014/CNB-INDECOPI .

Ambas normas técnicas peruanas, la NTP ISO/IEC 27001 y la NTP ISO/IEC 17799, están basadas en la familia de normas ISO 27000 correspondiente a seguridad de la información. La primera, es el estándar principal de esta familia y menciona cuales son los requerimientos para desarrollar un sistema de gestión de seguridad de la información basándose en el ciclo de DEMING, o ciclo Plan – Do – Check - Act, una metodología cíclica muy usada en las normas ISO relacionadas a normas de gestión [NTP ISO/IEC 27001].

OBJETIVO

El objetivo del manual es definir claramente el propósito de implementación de Gestión de Seguridad de los sistemas informáticos, redes, servidores y usuarios finales.

ALCANCE

El presente manual se aplica en todas las actividades realizadas en la implementación del Sistema de Gestión de Seguridad de la Información del Gobierno Regional de Huancavelica.

Gobierno Regional
HUANCAVELICA

DOCUMENTOS DE REFERENCIA

- ✓ Ley Marco de Modernización de la Gestión del Estado-ley 27658.
- ✓ la ley N2 29733- ley de Protección de datos personales para garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.
- ✓ Técnicas seguridad sistemas de gestión de seguridad de la información requisitos".
- ✓ Resolución de la Secretaría General de la República N° 007 2015-DP-SGPR en la que se designa Oficial de Seguridad de la Información del Despacho Presidencial.

Evaluación del valor de riesgo.

Una vez identificados los riesgos, se procederá a evaluar, junto con los dueños de los procesos, cuáles son las probabilidades de ocurrencia y los impactos que traerían a la organización en caso se materialicen estos riesgos, para ello podrán usar las escalas desde "Muy Baja" hasta "Muy Alta" para las probabilidades y una escala de "Insignificante" hasta "Catastrófica" para el impacto.

GOBIERNO REGIONAL Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

1. CLASIFICACIÓN DE LA INFORMACIÓN

La información debe ser clasificada de acuerdo con el nivel de sensibilidad, y los requerimientos legales y de privacidad.

1.1 RESPONSABLES POR LA INFORMACION

Los responsables por la información serán los encargados de clasificar, proteger y autorizar el acceso a la información del Gobierno Regional de Huancavelica , que se encuentre bajo su responsabilidad y de asegurar que los usuarios internos y externos tengan acceso a todos los datos y aplicaciones siempre que sea necesario.

INFORMACIÓN: Datos dotados de significado y propósito, desempeña un papel fundamental en todos los aspectos del modelo de negocios para el Gobierno Regional de Huancavelica, siendo el componente más indispensable de la institución.

La información debe ser clasificada por los respectivos responsables siguiendo las normas establecidas para la clasificación. En este caso tales responsables asumen el papel de tutores de la información, en tanto la propiedad será siempre del Gobierno Regional de Huancavelica.

La información debe ser clasificada en alguno de los siguientes niveles:

Pública o no clasificada	**NCI0**	Información de uso interno y/o externo, con controles mínimos cuya divulgación no tiene impacto sobre el Gobierno Regional de Huancavelica.
Interna	**NCI1**	Información con el propósito de distribución dentro del Gobierno Regional de Huancavelica, la fuga divulgación de esta información podría causar un daño mínimo a la imagen y/o reputación del Gobierno Regional de Huancavelica si fuera accedida por terceras partes.
Confidencial	**NCI2**	Información que está sujeta a acceso específicamente autorizado y su distribución es controlada, ya sea por personal funcionarios o contratados. Todo el personal con acceso a esta información debe utilizarla para realizar sus tareas diarias de forma efectiva. La divulgación fuga, adulteración, robo no autorizado de la información NCI2 podría dañar la imagen y/o reputación del Gobierno Regional de Huancavelica severamente y/o conducir a problemas tangibles o intangibles cruciales.
Distribución Restringida	**NCI3**	Información con el más alto grado de confidencialidad, la cual si es divulgada sin autorización, podría causar daños económicos y materiales significativos o hasta poner en riesgo la viabilidad de los funcionarios del Gobierno Regional de Huancavelica. La asignación de la clasificación de NCI3 debe ser autorizada por un directivo relevante en cada caso individualmente.

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Sistemas de Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

INFORMACION PÚBLICA O NO CLASIFICADA (NCI0)

Información de uso interno y/o externo, con controles mínimos, cuya divulgación no tiene impacto sobre el Gobierno Regional de Huancavelica.

Es toda información cuyo conocimiento y uso están restringidos al ambiente interno y al propósito del gobierno. Es puesta a disposición del trabajador o funcionario y puede ser revelada al público externo previa autorización de sus responsables.

1.2. INFORMACIÓN DEL USO INTERNO (NCI1)

Información con el propósito de distribución dentro del Gobierno Regional de Huancavelica, la fuga, divulgación de esta información podría causar un daño

mínimo a la imagen y/o reputación del Gobierno Regional de Huancavelica si fuera accedida por terceras partes.

La información NCI1 puede incluir lo siguiente:

- ✓ Informes
- ✓ Solicitudes
- ✓ Memorandos
- ✓ Resoluciones
- ✓ Etc.

1.3. INFORMACIÓN DE DISTRIBUCIÓN CONFIDENCIAL (NIC2)

Información que está sujeta a acceso específicamente autorizado y su distribución es controlada, ya sea por personal nombrado, funcionarios o contratados.

Todo el personal con acceso a esta información debe utilizarla para realizar sus tareas diarias de forma efectiva. La divulgación, fuga, adulteración, robo no autorizado de la información NCI2 podría dañar la imagen y/o reputación del Gobierno Regional de Huancavelica severamente y/o conducir a problemas tangibles o intangibles cruciales.

A continuación se incluyen ejemplos de información clasificada como NIC2:

- ✓ Cheques.
- ✓ Procedimientos internos.
- ✓ Cotizaciones.
- ✓ Entre otros.

1.4. INFORMACIÓN DE DISTRIBUCIÓN RESTRINGIDA (NIC3)

Información con el más alto grado de confidencialidad la cual si es divulgada sin autorización, podría causar daños económicos y materiales significativos o hasta poner en riesgo la viabilidad de los funcionarios del Gobierno Regional de Huancavelica. La asignación de la clasificación de NCI3 debe ser autorizada por un directivo relevante en cada caso individualmente.

Su conocimiento debe limitarse a un número reducido de personas autorizadas formalmente. Esa información exige medidas especiales de control y protección contra accesos o copias no autorizadas.

La información secreta en general está limitada a los trabajadores o funcionarios designados previamente por los responsables que, de acuerdo con la naturaleza de la función que ejercen, están obligados a conocerla.

Como regla general la información clasificada como NIC3 no debe ser almacenada en computadoras portátiles. En el caso en que esto sea necesario, los trabajadores y funcionarios deben reforzarse para limitar la existencia de los archivos con información secreta en sus computadoras personales a los

proyectos o trabajos en cursos y eliminarla inmediatamente luego concluir dichas tareas.

En ausencia de clasificación, toda información deberá considerarse NIC3.

A continuación se incluyen ejemplos de información clasificada como NIC3:

- ✓ Accesos a la plataforma e información del SEACE.
- ✓ Contraseñas de sistemas y registros financieros.
- ✓ Contraseñas de equipos networking, seguridad informática, sistemas web, sistemas informáticos.
- ✓ Recursos directamente recaudados.
- ✓ Detalles técnicos sobre proyectos en desarrollo o ya desarrollados por la institución.

2. PROPIEDAD DE LOS RECURSOS Y DE LA INFORMACIÓN

Es importante ser consciente de la propiedad de los recursos y de la información que son utilizados para el cumplimiento de las tareas y objetivos de cada oficina del Gobierno Regional de Huancavelica, teniendo esto en cuenta es importante cumplir con las siguientes reglas:

- ✓ Recursos tales como, impresoras, computadoras, copiadoras, software e información en cualquier formato o medio, son propiedad del Gobierno Regional de Huancavelica y serán puestos a disposición de los trabajadores y funcionarios de acuerdo con sus necesidades específicas de conocimiento y uso, por el tiempo determinado que sea necesario o horizonte de su contrato, siendo el trabajador y funcionario totalmente responsable por la seguridad de los mismos.
- ✓ Los recursos del Gobierno Regional de Huancavelica deben utilizarse solamente para fines relacionados a las tareas y objetivos de cada oficina.
- ✓ Los recursos de propiedad del Gobierno Regional de Huancavelica deben utilizarse observando siempre las reglas y condiciones de uso descritas en los procedimientos de la oficina de bienes patrimoniales.
- ✓ Las contraseñas de acceso a los sistemas del Gobierno Regional de Huancavelica (correo electrónico, Internet, Intranet, SIAF, SIGA o cualquier otra contraseña de acceso) deben mantenerse en secreto y no deben proporcionarse a ninguna otra persona que no sea trabajadores y funcionarios autorizados por la Sub gerencia de Desarrollo Institucional y TI. El trabajador y/o funcionario debe procurar que nadie pueda utilizar los sistemas del Gobierno Regional de Huancavelica haciéndose pasar por él. Recuerde que su contraseña garantiza el acceso a la información y sistemas de la institución y que si otras personas logran obtenerlas, tendrán acceso según el nivel de acceso que posee, y el registro que quedará de las operaciones realizadas serán del dueño de la contraseña (o sea el suyo) y no de la persona que efectivamente hizo uso de ella.
- ✓ Utilice la información y los recursos del Gobierno Regional de Huancavelica en estricto cumplimiento de la legislación vigente sobre los derechos del autor y la ley de protección de datos personales.

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

- ✓ Los sistemas de administración de correos electrónicos y todos los mensajes creados por los mismos, incluyendo las copias de backup de estos mensajes, son considerados propiedad del Gobierno Regional de Huancavelica.
- ✓ El contenido de las informaciones creados por los sistemas de información y comunicación y enviados por medio de recursos de propiedad del Gobierno Regional de Huancavelica, debe cumplir estrictamente con las políticas y los fines de la institución.
- ✓ La entidad se reserva el derecho de, sin aviso previo examinar las comunicaciones electrónicas con motivos estadísticos u otros y se reserva el derecho de utilizar herramientas automatizadas de monitoreo y búsqueda de palabras o patrones que puedan indicar uso abusivo.
- ✓ El contenido y uso de las comunicaciones electrónicas pueden ser monitoreados para soportar actividades de mantenimiento, seguridad o investigación.
- ✓ El responsable por la información podrá verificar, en cualquier momento si las reglas de seguridad de la información de este manual están siendo cumplidas debidamente.
- ✓ Queda totalmente prohibido borrar la información y los recursos relacionados de propiedad del Gobierno Regional de Huancavelica, al momento de la finalización del contrato de cualquier trabajador o funcionario. La oficina de Gestión de Recursos Humanos y el jefe de la unidad orgánica a la cual el trabajador o funcionario perteneció, deben verificar que sean devueltos, en caso contrario será motivo de sanción.
- ✓ Cualquier tipo de fuga, robo de información que dañe la imagen y reputación del Gobierno Regional a entes terceros o personas que no tiene vínculo con la entidad, será causal para tomar las acciones legales necesarias y las sanciones de comprobarse la fuente del suceso.
- ✓ Esta expresamente prohibido utilizar los recursos del Gobierno Regional de Huancavelica para la distribución de información, archivos, publicación o ejecución de asuntos no relacionados del Gobierno Regional de Huancavelica, como por ejemplo material pornográfico de tinte racista, fotos, audio, chistes, cuentos, videos, música, tarjetas electrónicas, apuestas, juegos electrónicos (en software o a través de Internet), en cualquier formato digital.
- ✓ No se debe instalar en los equipos informáticos de la institución softwares no autorizados o sin licencia, solo aquellos bajo licencia y autorizados por la Oficina de Desarrollo Institucional y Tecnología de la Información Sub Gerencia Desarrollo Institucional y Tecnologías de Información del Gobierno Regional de Huancavelica.
- ✓ En caso de que sea necesario instalar algún "plugin" en el navegador (Internet Explorer), los colaboradores deberán verificar antes con Sub Gerencia Desarrollo Institucional y Tecnologías de Información y Soporte técnico local si realmente es necesario utilizarlo.
- ✓ Siempre que exista una actualización de MS-Windows referida a problemas de seguridad, los colaboradores deben verificar con Sub Gerencia Desarrollo Institucional y Tecnologías de Información y Soporte técnico la necesidad de realizar dicha actualización.
- ✓ La marca, el nombre y el logotipo de la institución solo pueden utilizarse con fines del trabajo y la prestación de servicios del Gobierno Regional de

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

Huancavelica. Para utilizarlos con otros propósitos, es necesaria la autorización previa del ente perteneciente al Gobierno Regional de Huancavelica (Oficina de Imagen Institucional).

3. DIVULGACIÓN DE INFORMACIÓN

Uno de los aspectos más relevantes de la seguridad de la información está relacionado con la actitud de las personas y la cultura organizacional en el cuidado respecto de la divulgación de la información. Uno de los riesgos principales relacionados con esa cuestión es el de "Ingeniería social" la cual es una técnica utilizada por personas malintencionadas con la finalidad de obtener información a la que normalmente no tendrían acceso, ya sea persuadiendo a colaboradores, inspeccionando papeles, gavetas, armarios y cestos de basura, u obteniendo acceso físico a lugares restringidos.

Por este motivo se debe tener las siguientes precauciones:

- ✓ No discutir asuntos confidenciales o internos pendientes del Gobierno Regional de Huancavelica fuera de los lugares de trabajo o en presencia de terceros que no estén directamente involucrados con dichos asuntos.
- ✓ No discutir asuntos pertinentes del Gobierno Regional Huancavelica con ninguna persona que no necesite tener conocimiento de esa información, tales como amigos, profesores, familiares, prensa, entre otros.
- ✓ No discutir asuntos pertinentes del Gobierno Regional de Huancavelica en áreas ajenas a la institución y principalmente, en áreas y lugares públicos, tales como ascensores, aeropuertos, taxis, restaurantes, parques, bares y aviones.
- ✓ Adoptar recaudos adicionales en lo que respecta a la seguridad, al manejar información y documentos pertenecientes al Gobierno Regional de Huancavelica en lugares públicos que presenten riesgos de exposición como los anteriormente citados.
- ✓ Solo utilizar la información del Gobierno Regional de Huancavelica para fines profesionales o de trabajo.
- ✓ No facilitar el acceso transmita o entregue a ninguna persona o entidad información, ya sea en forma escrita, impresa o en formato electrónico (mediante archivos, e-mail o internet), sin obtener la debida autorización del responsable por la información respecto de la divulgación del contenido y la forma en que será transmitido.
- ✓ No suministrar información de la institución a personas desconocidas o a quien no necesite conocerla y sin la respectiva autorización del responsable de la misma.
- ✓ Siempre adoptar una actitud reservada con personas que intenten obtener información personal colaborador o prestadores de servicios del Gobierno Regional de Huancavelica.
- ✓ Siempre solicitar más de una identificación como garantía y comprobación de la identidad de su interlocutor cuando trate asuntos

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V°B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

de la institución así como también algún dato de contacto por ejemplo, teléfono y dirección debidamente comprobada.

- ✓ Relatar inmediatamente a su superior cualquier incidente o sospecha de incidente de seguridad observado.
- ✓ No compartir información clasificada como NIC1, NIC2 o NIC3 en sus dispositivos personales móviles, como por ejemplo PDAs (Personal Digital Assistant), tarjetas de memoria y demás dispositivos que puedan almacenar información (USB).
- ✓ No divulgar información ni total ni parcialmente a otras personas que no sean trabajadores u funcionarios o que no estén directamente relacionadas y definidas formalmente por el Gobierno Regional de Huancavelica y sus sedes. La divulgación de información del Gobierno Regional de Huancavelica solamente debe efectuarse previa autorización por escrito y/o con motivo de exigencias legales o normativas.

4. DOCUMENTOS

Considere como documento, a toda información puesta a disposición por medio de los recursos del Gobierno Regional de Huancavelica, ya sea a través del correo electrónico, en archivos (físicos o electrónicos) o en papel. Nótese que estos pueden contener información clasificada con algunas de las categorías determinadas previamente (Clasificación de la información).

Cuando un documento no posea una clasificación claramente visible, avise inmediatamente a la Sub Gerencia Desarrollo Institucional y Tecnologías de Información Soporte técnico quien informara correspondientemente al comité de seguridad, para que se active los procedimientos correspondientes a fin de revertir la situación.

Teniendo en cuenta lo expresado anteriormente se deberá cumplir las siguientes reglas:

- ✓ No dejar documentos junto a impresoras, copiadoras después de su utilización. Acompañe todas las fases de los procesos de impresión, manejo y destrucción de los documentos clasificados como NIC2 o NIC3.
- ✓ Mantener todos los documentos y materiales de trabajo que contengan información del Gobierno Regional de Huancavelica en lugares adecuados para su almacenamiento y protegidos contra el acceso indebido, siguiendo las políticas de almacenamiento de datos establecidas por la Sub Gerencia Desarrollo Institucional y Tecnologías de Información no dejar documentos clasificados como NIC2 o NIC3 con su contenido visible y a la mano de terceras personas.
- ✓ Guardar todos los documentos y la información en gavetas o armarios cerrados y protegerlo su contenido de ser visualizado siempre que se aleje de su lugar de trabajo independientemente del tiempo que estará alejado.
- ✓ No utilizar recordatorios escritos (como contraseñas u otros accesos) que expongan información confidencial al ambiente externo (monitor,

escritorio, etc).

- ✓ Organizar los papeles de trabajo y los documentos importantes y clasificados en archivadores de acuerdo con los procedimientos ya existentes y estipulados por el Gobierno Regional de Huancavelica para el cierre de año para que sean almacenados en los archivos periféricos y posteriormente derivados al archivo central.
- ✓ Cuando exista la necesidad de eliminar documentos que contengan información clasificada como NIC1, NIC2 o NIC3, destrúyalos de forma tal que su contenido sea irrecuperable. En cuanto a los datos en formato electrónico, verifique que los mismos hayan sido eliminados completamente, (por ejemplo. Vaciado de la papelera de reciclaje en MS-Windows o usar las teclas "Shift + Supr")
- ✓ Verificar cuidadosamente a los destinatarios de la correspondencia para evitar errores en la entrega y por consiguiente el desvío de información tanto por medio convencionales como electrónicos.
- ✓ Cuando se envía información confidencial por el correo o mensajeros, utilizar un protocolo de recepción que contenga los siguientes campos: nombre, documentos de identidad, cargo, dependencia, fecha y horario de envío y de entrega.
- ✓ Utilizar solo servicios seguros, aprobados y confiables por el Gobierno Regional Huancavelica para el transporte de documentos.

5. ACCESO DE IDENTIFICACION DE PERSONAS

El acceso a las oficinas del Gobierno Regional de Huancavelica debe ser restringido a las personas no autorizadas, a fin de evitar el riesgo de acceso indebido a la información y a los recursos del Gobierno Regional de Huancavelica. En virtud de ello deben seguirse las siguientes reglas:

- ✓ El personal de seguridad debe dar una identificación a cualquier persona que no pertenezca a la institución.
- ✓ Estar siempre atento a cualquier persona extraña que circule en las oficinas del Gobierno Regional de Huancavelica.
- ✓ Comunicar a la central de seguridad (vigilancia) la presencia de personas extrañas al ambiente de trabajo o que no se encuentren debidamente identificadas.
- ✓ Todas las personas que sean trabajadores y funcionarios del Gobierno Regional de Huancavelica deben portar su **tarjeta de identificación** (fotocheck) durante toda su jornada laboral y quedar debidamente registrada en la base de datos de los sistemas de control biométricos de la oficina Gestión de Recursos Humanos y las cámaras de video vigilancia.
- ✓ Todas las personas naturales y jurídicas que estén visitando las oficinas del Gobierno Regional de Huancavelica deben portar su **tarjeta de acceso** (fotocheck) durante toda su permanencia y quedar debidamente registrada en la bitácora de visitante de la oficina de vigilancia tanto como las cámaras de video vigilancia.
- ✓ En caso de poseer tarjeta de accesos o identificación personal para el ingreso al edificio, se deberán cumplir las siguientes reglas:

a. El personal o funcionarios deben de llevar la tarjeta de identificación personal en un lugar visible siempre.

b. La tarjeta de identificación es un instrumento de uso personal e intransferible por lo que no debe utilizarse para fines que no sean identificación ni prestarse a ninguna otra persona bajo ningún pretexto. La conservación adecuada de la tarjeta de identificación es responsabilidad de cada trabajador y/o funcionario.

c. En caso de pérdida o robo de la tarjeta de identificación, comunique el hecho inmediatamente a la Oficina de Gestión de Recursos Humanos.

d. Las tarjetas de identificación de uso temporal deben ser devueltas al personal de control (vigilancia), cuando el portador deje las oficinas del Gobierno Regional de Huancavelica.

e. La tarjeta de acceso provisional solamente podrá entregarse cuando el trabajador se olvide la original y deberá ser entregado con la autorización previa de la Oficina de Gestión de Recursos Humanos.

6. CORREO ELECTRÓNICO (e-mail)

El correo electrónico es un medio importante de comunicación y transmisión de datos sin embargo si se utiliza incorrectamente puede causar serios daños a la institución por este motivo se cumplirán las reglas definidas a continuación:

- ✓ El uso de correo electrónico es obligatorio para todo trabajador o funcionario.
- ✓ Las cuentas empiezan con la inicial de su primer nombre y su primer apellido acompañado luego del @ y respectivo dominio.
- ✓ En caso de coincidir con la inicial y el primer apellido la cuenta será acompañada de la segunda inicial de su apellido ejemplo: ctorres@regionhuancavelica.gob.pe, el otro correo será ctorresz@regiohuancavelica.gob.pe
- ✓ El tamaño de la cuenta es de 5gb para usuarios y 10g para directores (funcionarios), en caso de utilizar más recursos para almacenamiento debe comunicarse a la Sub Gerencia Desarrollo Institucional y Tecnologías de Información para que se tome acciones e incrementar el tamaño de la cuenta.
- ✓ La comunicación por correo electrónico entre trabajadores y funcionarios es obligatoria la Subgerencia Desarrollo Institucional y Tecnologías de Información se encargará de establecer la tecnología del correo electrónico así como los backups respectivos; no utilizar cuentas personales de correo electrónico para comunicarse o para transmitir cualquier otro tipo información relacionado a la institución.
- ✓ Al intercambiar correos electrónicos con personas naturales, jurídicos y terceros el contenido de los mensajes podrá ser considerado como la posición oficial de la institución por lo tanto actué con seriedad y profesionalismo.
- ✓ No transmitir por correo electrónico a otras cuentas de correo electrónico fuera

del ambiente de Gobierno Regional de Huancavelica archivos anexados que contengan información clasificada como NIC2 o NIC3. En caso que sea necesario el envío de correo electrónico de algún documento o archivo que contenga este tipo de información se debe obligatoriamente protegerse para evitar la lectura indebida utilizando una contraseña de la aplicación en que lo generó como por ejemplo una contraseña de Winzip, Winrar, 7-Zip, Word, Excel etc, o alternativamente, algún recurso criptográfico disponible en la institución. Nunca envíe en el mismo correo electrónico un mensaje protegido y las contraseñas o claves cristológicas utilizadas.

- ✓ No enviar mensajes internos o externos que pueden perjudicar la imagen y/o reputación del Gobierno Regional de Huancavelica tales como: chistes, material de carácter sexual, imágenes videos con extensiones .mpeg .avi u otras, música .mp3, .wav u otras, juegos, mensajes o textos de contenido étnico, criminal, religioso, político o que pueda interpretarse como inofensivo.
  - ✓ Cualquier correo identificado que se haga envío de SPAM primeramente será amonestado formalmente, y de reiterarse será deshabilitado.
  - ✓ No crear ni reenviar cadenas de correo electrónico en las cuales el receptor es inducido a enviar mensajes a otras personas sin que haya una necesidad profesional.
  - ✓ Proteja contra alteraciones indebidas los documentos confidenciales en formato electrónico que deban enviarse. Para ello conviértalos a formatos que no permitan la alteración del contenido como por ejemplo .pdf (Acrobat Reader - Foxit Reader) siempre verificando que el archivo fue configurado con protección contra copia, edición o impresión en caso de ser requerido.
  - ✓ Estar atento para que los mensajes sean enviados a los destinatarios pretendidos y solo a ellos, asegúrese de que la dirección de correo electrónico sea correcta evitando así que cualquier información sea dirigida a destinatarios incorrectos.
  - ✓ Tener en cuenta que todos los correos electrónicos enviados o recibidos por el sistema de correo electrónico de la institución pueden ser abiertos y analizados por el Gobierno Regional de Huancavelica sin previo aviso.
  - ✓ Verificar la presencia de virus en todos los archivos anexados a los correos electrónicos antes de abrirlos.
  - ✓ No lea, acceda, ni divulgue correos electrónicos de otros trabajadores y funcionarios sin la debida autorización.
  - ✓ Este atento al tamaño máximo de archivos anexos para la transmisión por correo electrónico a fin de evitar problemas en el sistema de correo electrónico, o incluso la suspensión todo el servicio de mensajes de la institución.
  - ✓ Las casillas de correo electrónico puesta disposición por el Gobierno Regional de Huancavelica tienen un tamaño limitado por lo tanto verificar que siempre se encuentre dentro de los límites establecidos transfiriendo toda la información referida a trabajos a los respectivos archivos técnicos.

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

7. TELEFONÍA

Los recursos de telefonía son puestos a disposición para tratar asuntos relacionados con las actividades del Gobierno Regional de Huancavelica pueden ser usados para asuntos personales de forma moderada. Estos recursos pueden presentar riesgos para seguridad de la información por lo que se requieren una atención especial en base a lo mencionado se deberán cumplir las siguientes reglas.

- ✓ Tener cuidado al dejar a una persona esperando en línea con el teléfono descolgado permitiendo que oiga asuntos confidenciales del Gobierno Regional de Huancavelica, si no puede postergar la llamada ni interrumpir la conversación con su interlocutor, presione la tecla "**MUTE**" del teléfono.
- ✓ Utilice el recurso de "**MANOS LIBRES**" (o speaker) modernamente para evitar que otras personas escuchen la conversación y tomen conocimiento del asunto discutido.
- ✓ Evite utilizar los teléfonos celulares para discutir en lugares públicos asuntos confidenciales del Gobierno Regional de Huancavelica pues otras personas podrían estar oyendo su conversación. Por otra parte siempre existe la posibilidad de que la comunicación por celulares sea interceptada especialmente cuando están en modo analógico.
- ✓ Al dejar recados en contestadores automáticos o casillas de correo solamente trasmita la información necesaria para que la otra persona pueda devolver la llamada (por ejemplo, nombre y teléfono de con tacto) evitando suministrar información detallada sobre el asunto a ser tratado pues estos aparatos y servicios pueden interceptarse.
- ✓ Al atender su teléfono no divulgar más información que su nombre y el nombre del Gobierno Regional de Huancavelica excepto cuando total certeza de la identidad y las intenciones de su interlocutor.
- ✓ No discutir asuntos confidenciales con interlocutor desconocido o con propósitos dudosos por teléfono o personalmente verifique primero la identidad y los propósitos del interlocutor.
- ✓ Evite utilizar teléfonos para discutir asuntos confidenciales del Gobierno Regional de Huancavelica y si esto fuera indispensable hágalo de forma discreta asegurándose de la conversación no esté siendo oída por otras personas.

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

8. VIRUS

Los virus son programas nocivos desarrollados para causar algún tipo de daño a los archivos, sistemas o redes de computadoras, así como también para capturar información o utilizar su equipo como base para dañar o acceder otros equipos de redes. Los virus pueden ser introducidos por medio de un archivo anexado al correo electrónico, un usb infectado, una configuración inadecuada en el sistema operativo de su equipo o inclusive a través de archivos obtenidos en internet.

Para minimizar el riesgo de que los sistemas informáticos del Gobierno Regional

de Huancavelica sean perjudicados por un virus se debe cumplir las siguientes reglas:

- ✓ Mantener siempre el antivirus actualizado (sophos central Intercept X Advanced).
- ✓ Si no tuviera instalado su antivirus exija a Soporte técnico que lo instalen.
- ✓ El antivirus estará programado para realizar un scan en horas de almuerzo, principalmente para que no interrumpa su trabajo una vez por semana si tiene duda contacte con Soporte técnico.
- ✓ Es necesario que realice un scan del equipo (PC y laptop) principalmente cuando alguna de las siguientes condiciones sea aplicable a su equipo:

  a. Recién adquirido.

  b. Prestado.

  c. Al introducir un USB

  d. Recién llegado el servicio de mantenimiento.

  e. Al regresar de utilizar un seminario, exposición, charla, etc.

  f. Utilizado para propósitos que puedan haberlo expuesto a ser infectado por virus.

- ✓ En caso de que no sea posible conectarse a la red del Gobierno Regional de Huancavelica para actualizar el antivirus póngase en contacto con Soporte técnico para coordinar dicha tarea.
- ✓ No abra correos electrónicos de remitentes desconocidos (adjuntados extraños y reportados por el correo) o que sean probables portadores de virus.
- ✓ En caso de duda en relación con los equipos o archivos que puedan contener virus, contáctese con soporte técnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información.
- ✓ En caso de problemas con el software de antivirus, no desinstale inhabilite, ni intente reconfigurarlo. En estos casos contáctese inmediatamente con Soporte técnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información.
- ✓ Verifique el software y los archivos utilizados, o que serán utilizados en las computadoras y la red del Gobierno Regional de Huancavelica en relación con la existencia de virus siempre que:
  a. Vaya enviarlo a otra apersona.
  b. El software fue recientemente adquirido.
  c. Que haya descargado archivos de internet o de otras fuentes.
  d. El software o archivos hay sido recibido de un externo USB), vendedores, etc
- ✓ Borre los archivos temporarios creados después del acceso a Internet por medio de acceso telefónico (dial up) o cualquier otra conexión fuera de la red Gobierno Regional de Huancavelica.

- ✓ No instale ningún software que no esté autorizado y posea una licencia obtenida por Gobierno Regional de Huancavelica. En caso de que necesite instalar en navegador (Internet Explorer) algún complemento o "plugins", verifique antes con Soporte técnico si realmente es necesario utilizarlo y si la versión es la autorizada por el Gobierno Regional de Huancavelica. La instalación de algunos programas de software o "plugins" puede hacer que su máquina sea vulnerable a ataques para la implantación de virus u otras acciones nocivas.

9. SEGURIDAD LÓGICA

La información del Gobierno Regional de Huancavelica debe ser protegida en los medios de almacenamiento electrónico, tales como computadoras, de CD, DVD y USB.

Para ello se debe seguir estas reglas:

- ✓ Mantenga el recurso de protección de pantalla (salva pantallas) protegido por contraseña. El protector de pantalla debe estar configurado para activarse en un máximo de 5 (cinco) minutos de inactividad del computador. Bloquee manualmente su id de Windows (Crtl + Alt + Supr) cuando esté alejado de su puesto de trabajo.
- ✓ Siempre que los recursos disponibles lo permitan utilizar algún tipo de encriptación y protejer con contraseña los archivos con información confidencial (Comprimido con winrar, contraseña a office, etc).
- ✓ No compartir archivos, directorios o unidades de disco en las notebooks y desktops.
- ✓ No permitir que otras personas utilicen su computadora sus conexiones de red, servicios de Internet y otros recursos.

GOBIERNO REGIONAL HUANCAVELICA
Sub Gerencia de Desarrollo Institucional Tecnologías de la Información
Ing. Cesar J. Altamirano Flores

10. CONTRASEÑAS

La contraseña es el método más comúnmente utilizado para autentificar al usuario y para proteger su información, evitando el acceso no autorizado a recursos, archivos y sistemas que puedan ser dañados o utilizados indebidamente. Recuerde que la responsabilidad por las acciones efectuadas en los sistemas durante una sesión autentificada con su contraseña le será atribuida a ud.

Cumplir las siguientes reglas a efectos de la protección de la información.

- ✓ Defina contraseñas compuestas por letras entre mayúscula y minúscula, números, caracteres especiales permitidos con tamaño mínimo de 8 (ocho) caracteres.
- ✓ No relaciones sus contraseñas con información personal tal como su nombre de usuario nombre de algún familiar, número funcional departamento número de DNI, fecha de nacimiento, equipo de futbol, etc.

- ✓ No divulgue sus contraseñas a otras personas ya que las mismas constituyen su llave de acceso de uso personal e intransferible no anotar en papeles recordatorios, archivos electrónicos o en otros lugares (postfix pegado en el monitor).
- ✓ No adopte la misma contraseña para más de una aplicación.
- ✓ Modifique su contraseña temporalmente en el primer acceso al sistema.
- ✓ No utilice recursos provistos por Windows o por cualquier otro software que permitan el almacenamiento de contraseñas para uso futuro.
- ✓ En caso de tener acceso a sistemas, programas de software o redes en lugares o equipos fuera del Gobierno Regional de Huancavelica, no utilice ninguna de las contraseñas que utiliza normalmente en los sistemas del Gobierno Regional de Huancavelica.
- ✓ En caso de tener que enviar archivos protegidos por contraseña no utilice ninguna de las contraseñas que utiliza normalmente para acceder a los sistemas del Gobierno Regional de Huancavelica aun cuando esos archivos sean utilizados internamente.
- ✓ Si algún mensaje sospechoso solicita el cambio de su contraseña ya sea por correo electrónico o por pantalla de su computadora verifique con soporte técnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información de la veracidad de la solicitud antes de realizar los procedimientos de cambio.
- ✓ Cambie sus contraseñas dentro de un máximo de 90 (noventa) días, aun cuando el sistema no lo exija en el momento del cambio, no utilice las últimas 10 (diez) contraseñas adoptadas anteriormente.
- ✓ Si su cuenta de usuario se encuentra bloqueada contáctese con soporte tecnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información y procure identificar el motivo de bloqueo ya que personas no autorizadas pueden estar intentando utilizarla indebidamente.
- ✓ Si informa sus contraseñas cuando su computadora es enviada al servicio técnico solicite cambiar sus contraseñas divulgadas inmediatamente después del mantenimiento del equipo.
- ✓ Cambie inmediatamente sus contraseñas si sospecha que otras personas tomaron conocimiento de ellas, si sospecha que se obtuvo información o se efectuaron acciones no autorizado en su nombre comuníquelo a soporte técnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información.

GOBIERNO REGIONAL * Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información * V° B° Ing. Cesar J. Altamirano Flores * HUANCAVELICA

11. DESKTOPS Y NOTEBOOKS

Las notebooks son blanco de frecuente de robos en virtud de su alto valor en el mercado y del valor estratégico de la información contenida en estos equipos por ello cumpla las siguientes reglas tanto para las notebooks como para las desktops:

- ✓ Siempre asegure su notebook con el cable candado de seguridad provisto por el Gobierno Regional de Huancavelica tanto cuando su equipo se encuentre desatendido como cuando usted esté trabajando con él. Esta precaución deberá ser tomada dentro de las instalaciones del

Gobierno Regional de Huancavelica o fuera de las mismas.

- ✓ Si sale con el equipo para cualquier evento programado u otro evite andar con el equipo del Gobierno Regional de Huancavelica por lugares peligrosos y sospechosos.
- ✓ Siempre mantenga sus datos en forma encriptado y con contraseñas difícil de adivinar.
- ✓ Nunca preste su equipo a otras personas.
- ✓ Verifique que los maletines o bolsos utilizados para el transporte de su notebook se encuentren en condiciones y sean adecuados para garantizar la protección física del equipo.
- ✓ En caso de robo o hurto de la notebook comuníquelo inmediatamente a la oficina de patrimonio y registre su denuncia respectiva en una comisaria.
- ✓ No permita que nadie pueda hacer cambios internos de componentes de hardware de su notebook o desktop así como (Memoria RAM, disco duro, Microprocesador entre otros)
- ✓ En caso de hacer un mantenimiento preventivo y correctivo, recurra al soporte técnico - La Sub Gerencia Desarrollo Institucional y Tecnologías de Información es la única área autorizado para realizar cambios dentro de su notebook o desktop.
- ✓ Guarde su información en la unidad "D" dentro de su Notebook o Desktop, ya que si se ve afectado por cualquier contingencia cambio de dominio, infección de virus, desconfiguración, etc no pierda su información. Si existirá perdida de información irrecuperable el único responsable es el usuario
- ✓ Realice backup (copia) y borre la información de la notebook o desktop enviada al servicio de soporte técnico, procurando proteger la información que contiene el equipo.
- ✓ No instale en su equipo software sin licencia la Sub Gerencia Desarrollo Institucional y Tecnologías de Información realizará periódicamente un inventario de todo el software instalado en el equipo, y el mismo deberá coincidir con el instalado originalmente para cumplimiento de sus funciones.
- ✓ La Sub Gerencia Desarrollo Institucional y Tecnologías de Información se reserva el derecho de auditar periódicamente todos los equipos provistos por el Gobierno Regional de Huancavelica o instalados dentro de sus oficinas sin previo aviso.
- ✓ En caso de que sea necesaria una mudanza física de una desktop, impresora u otro equipo comuníquelo a soporte técnico - La Sub Gerencia Desarrollo Institucional y Tecnologías de Información para que solicite su aprobación.
- ✓ Antes de conectar equipos de un prestador de servicios en la red del Gobierno Regional de Huancavelica, el colaborador responsable por ese prestador de servicios debe contactarse con el personal de la Sub Gerencia Desarrollo Institucional y Tecnologías de Información y solicitar su análisis y aprobación.

13. BACKUP

El backup es una copia de seguridad de los datos originales trasmitidos por los usuarios y almacenados en nuestros servidores, la cual es elaborada con el propósito de asegurar la disponibilidad de la información en caso de error o daños en los datos originales por ello deben adoptarse de las siguientes reglas:

- ✓ Tenga cuidado al almacenar archivos e información en la red del Gobierno Regional de Huancavelica en directorio públicos, incluso temporariamente ya que cualquier persona autorizada o no con acceso a la red de Gobierno Regional de Huancavelica podría acceder a esa información.
- ✓ Almacene todos los archivos relacionados con el trabajo que está siendo efectuado en un archivo comprimido con contraseña preferente en la unidad "D" del equipo, en caso de tener dudas comunicarse con soporte técnico - La Sub Gerencia Desarrollo Institucional y Tecnologías de Información.
- ✓ Utilice una herramienta para compactar datos antes de almacenar información.
- ✓ Está totalmente prohibido el almacenamiento de archivos de imagen, de video, de música, panfletos con apología etc. en la red del Gobierno Regional de Huancavelica.
- ✓ En caso de que sea necesaria la realización de backups especiales además de los ya efectuados en forma periódica comunicarse con soporte técnico - la Sub Gerencia de Desarrollo Institucional y Tecnologías de Información.

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

14. INTERNET

Internet es una herramienta muy útil para la investigación trabajo y el intercambio de información relevante a las funciones y objetivos del Gobierno Regional de Huancavelica, sin embargo y dado que no es difícil de interceptar mensajes electrónicos no hay garantía de que estas comunicaciones sean privadas.

Los usuarios también deben ser conscientes que muchos sitios Web emplean técnicas (Ej. Cookies, java applets, componentes ActiveX, etc) diseñados para entablar relación directa con su PCs, registrar preferencias del usuario o relevar información personal, cuando se accede una función particular de una página Web estos instrumentos son descargados desde el servidor Web al cliente y ejecutados en la PC del usuario; estos programas pueden ser configurados para enviar información del usuario hacía internet sin la participación o conocimiento del mismo.

14.1 USO ADECUADO DEL INTERNET

Internet es un activo del Gobierno Regional de Huancavelica suministrado a los trabajadores y funcionarios para contribuir con los objetivos de la

Gobierno Regional
HUANCAVELICA

institución, el uso personal ocasional o eventual de este recurso es permitido, en tanto no interfiera con la productividad del personal y no cause conflictos con la actividad, toda información trasmitida por este medio será tratada como información relacionada con los objetivos de la institución y debe estar alimentada a las normas y directivas, las restricciones sobre uso **no-productivo** sobre los usuarios serán aplicables por la Sub Gerencia Desarrollo Institucional y Tecnologías de Información.

Los usos estrictamente prohibidos de Internet corresponden, páginas que están restringidas a los que se presentan a continuación.

- ✓ Acceso a sitios Web relacionados con actividades de juego, apuestas o actividades ilegales en general.
- ✓ Acceso a material pornográfico o a sitios Web de contenidos para adultos relacionados con desnudismo, erotismo o pornografía.
- ✓ Acceso a sitios de música, juegos, videos u otros sitios de entretenimiento on- line.
- ✓ Accesos a sitios web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, profanidad, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.
- ✓ Accesos a sitios "Hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información del Gobierno Regional de Huancavelica.
- ✓ Descarga desde internet de cualquier material (incluyendo software ilegal) protegido bajo leyes de derecho de propiedad o archivos electrónicos para usos no relacionados con los objetivos de la institución, la descarga de software solo será permitida si el mismo está relacionado con los objetivos de la institución y siempre que cumplan las siguientes condiciones.
    a. *Debe ser autorizada por su jefe inmediato*
    b. *La autenticidad del software debe ser comprobada.*
    c. *Han sido investigadas y determinadas las condiciones para su uso (incluyendo tarifas de shareware), y estas condiciones han sido cumplidas.*
    d. *El software se instale de acuerdo a las políticas de seguridad mencionadas en este presente.*
    e. *El software fue examinado por una versión actualizada del antivirus de la institución*
- ✓ Publicación de comentarios negativos no profesionales del Gobierno Regional de Huancavelica en sitios personales, redes sociales, correo electrónico, o cualquier otro medio de publicación en Internet.
- ✓ Participación en cualquier actividad ilegal o criminal que involucre el uso de Internet.
- ✓ La Sub Gerencia Desarrollo Institucional y Tecnologías de Información monitorea todos los accesos a Internet, por lo tanto, esta herramienta deberá ser utilizada modernamente cuando se trate de asuntos no relacionados con los objetivos del Gobierno Regional de Huancavelica.
- ✓ Una vez se detecte el uso indebido del Ancho de Banda por

GOBIERNO REGIONAL * Gerencia de Desarrollo Institucional y Tecnologías de la Información * Vº Bº ..... Ing. Cesar J. Altamirano Flores * HUANCAVELICA *

aplicaciones no permitidas como con las VPN, proxies anónimos, Peer-to-peer, etc. Será automáticamente bloqueado sin tener acceso a Internet y posteriormente informar sobre su accionar a su jefe responsable y a la oficina de Recursos Humanos para ser sancionado.

15. REDES SOCIALES

- ✓ Al usar el internet del Gobierno Regional de Huancavelica para usar redes sociales queda totalmente prohibido compartir en grupos o de forma personal material de tipo pornográfico, xenofóbico, terrorismo, hacking, prejuicios, acoso explicito etc. que podría causar daños a la imagen de la Institución o entes relacionados a este siendo así el caso será bloqueado el acceso al origen de dichos mensajes y reportado para su sanción respectiva a la oficina Gestión de Recurso Humanos.
- ✓ Prestar atención cuando publiquemos y subamos material con el uso del Internet del Gobierno Regional de Huancavelica.
  a. *Pensar muy bien qué imágenes, vídeos e información escogemos para publicar sin que afecte a la imagen del Gobierno Regional Huancavelica.*
  b. *No publicar nunca información privada que pueda perjudicar la imagen del Gobierno Regional Huancavelica.*
- ✓ Escoger cuidadosamente a nuestros amigos.
  a. *No aceptar solicitudes de amistad de personas que no conozcamos o perfiles falsos que puedan realizar ingeniería social.*
  b. *Verificar todos nuestros contactos de forma permanente.*
- ✓ Proteger nuestro entorno de trabajo y no poner en peligro nuestra reputación y la del Gobierno Regional de Huancavelica:
  a. *Al registrarnos en una red social, usar nuestra dirección de correo personal (**no el correo institucional**)*
  b. *Tener cuidado de cómo representamos en Internet a nuestra empresa u organización*
  c. *No mezclar nuestros contactos de trabajo con nuestros amigos*
  d. *No guardar nuestras contraseñas de accesos a la red, sistemas, computadoras pertenecientes al Gobierno Regional de Huancavelica en nuestro móvil*
  e. *Usar las funciones de seguridad de que disponga nuestro móvil para el uso de redes sociales con el internet del Gobierno Regional de Huancavelica.*
- ✓ Proteger nuestro teléfono móvil y la información guardada en él.
  a. *Tener cuidado con lo que publicamos sobre otras personas, instituciones, empresas, organismos, etc. con el internet de la entidad.*
- ✓ Informarnos del uso de las redes sociales.
  a. *Leer con atención y de principio a fin la política de privacidad y las condiciones y términos de uso de la red social que escojamos*
- ✓ Protegernos con la configuración de privacidad de cada red social.
  a. *Usar opciones orientadas a la privacidad (comprobar quién puede ver nuestras fotos, quién puede ponerse en contacto con nosotros y quién puede añadir comentarios)*
- ✓ Prestar atención a los servicios basados en la localización y a la información

GOBIERNO REGIONAL Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar J. Altamirano Flores HUANCAVELICA

de nuestro teléfono móvil.

a. *Desactivar los servicios basados en la localización geográfica cuando no los estemos usando y/o usemos el internet del Gobierno Regional de Huancavelica.*

16. EXCEPCIONES A LA SEGURIDAD

Determinados requerimientos de la institución exigen que se flexibilice la política de seguridad, en el caso de estas excepciones la justificación deberá enviarse al personal asignado para tal fin las excepciones deben ser revisadas y renovadas en forma anual.

17. ¿CÓMO REPORTAR UN INCIDENTE DE SEGURIDAD?

Pueden reportar los incidentes de seguridad de la siguiente manera:

- ✓ Llamar a soporte técnico - Sub Gerencia Desarrollo Institucional y Tecnologías de Información, teléfono: (+51067) – 452891 anexo 1062-1063-1064.
- ✓ Enviar un correo a la siguiente dirección: soporte@regionhuancavelica.gob.pe.
- ✓ Contactar al responsable de Seguridad de TI.

GOBIERNO REGIONAL Sub Gerencia de Desarrollo Institucional y Tecnologías de la Información V° B° Ing. Cesar Altamirano Flores HUANCAVELICA

18. SANCIONES

La violación de un control de seguridad o el incumplimiento del manual de seguridad de la información del Gobierno Regional de Huancavelica, serán considerados infracciones cuya naturaleza y gravedad podrán implicar la aplicación de medidas disciplinarias de acuerdo con la gravedad de la infracción cometida por el trabajador o funcionario y el impacto causado por la misma podrán ser aplicadas las siguientes sanciones:

a. Pérdida de acceso a determinados recursos como por ejemplo correo electrónico, acceso a la red acceso a los sistemas del Gobierno Regional de Huancavelica.
b. La eliminación de información digital que ha sido producido por el servidor o funcionario en el desempeño de sus funciones mismo que se encuentra almacenada en el equipo de cómputo asignado, cual deberá de permanecer de forma intangible aun cuando haya culminado su vínculo laboral con la entidad o cuando haya sido desplazado a otras unidades orgánicas o dependencias.
c. Advertencia formal y escrita, dirigida a la oficina Gestión de Recursos Humanos.
d. Aplicación de sanciones laborales previstas en la legislación vigente de Perú.
e. Proceso civil o penal dependiendo de la legislación vigente de Perú.
f. Rescisión del contrato de prestación de servicios cuando sea aplicable.