Gobierno Regional Junín

RESOLUCIÓN GERENCIAL GENERAL REGIONAL

N°080-2020-GR-JUNIN/GGR

Huancayo, 22 ABR. 2020

EL GERENTE GENERAL REGIONAL DEL GOBIERNO REGIONAL JUNIN

VISTO:

El Informe Legal N° 0180-2020-GRJ/ORAJ del 20 de abril de 2020; Informe Técnico N° 06-2020-GRJ/GGR-ORDITI del 20 de abril del año 2020; Informe N° 008-2020-GRJ/GGR/ORDITI-JSM del 17 de abril del 2020; Manual de Seguridad de la Información;

CONSIDERANDO:

Que, de acuerdo al artículo 191° de la Constitución Política del Perú de 1993, modificada por la Ley N° 27680 – Ley de la Reforma Constitucional del Capítulo XIV, respecto a la descentralización, establece que: *"Los Gobiernos Regionales tiene autonomía política, económica y administrativa en los asuntos de su competencia (…)";*

Que, la autonomía de los Gobierno Regionales se define como la facultad de adoptar y concordar las políticas, planes y normas en los asuntos de su competencia, aprobar y expedir sus normas, decidir a través de sus órganos de gobierno y desarrollar las funciones que le son inherentes conforme a lo establecido en la Ley N° 27783 - Ley de Bases de la Descentralización;

Que, de acuerdo a lo prescrito en el inciso a) y d) del artículo 21° de la Ley N° 27867, es atribución del Presidente Regional, ahora llamado Gobernador Regional, según Ley N° 30305; de dirigir y supervisar la marcha del Gobierno Regional y de sus órganos ejecutivos, administrativos y técnicos, y dictar decretos y resoluciones regionales; asimismo, el referido precepto, lo reconoce como la máxima autoridad de la jurisdicción, representante legal y titular del Pliego Presupuestal del Gobierno Regional;

Que, de conformidad a lo dispuesto en el inciso b) del numeral 1., del artículo primero de la Resolución Ejecutiva Regional N° 018-2020-GRJ/GR del 27 de enero de 2020, se delega las facultades y atribuciones al Gerente General Regional;

Que, con Informe N° 008-2020-GRJ/GGR/ORDITI-JSM del 17 de abril de 2020, el Administrador de red del Gobierno Regional Junín y Seguridad Informática, remite adjunto el MANUAL DE SEGURIDAD DE LA INFORMACION (POLITICAS DE SEGURIDAD DE LA INFORMACION) al Director de la Oficina Regional de Desarrollo Institucional y Tecnologías de la Información (ORDITI);

Que, con Informe Técnico N° 06-2020-GRJ/GGR-ORDITI del 20 de abril de 2020, el Director Regional de Desarrollo Institucional y Tecnología de la Información, solicita en el tercer ítem la revisión y la aprobación por la instancia correspondiente, señalando en el ítem 1 y 2 del mismo que la propuesta del Manual de Seguridad de la Información se encuentra lista para la aprobación y se encuentra dentro de los parámetros establecidos, contando con el visto bueno de ORDITI;

GERENCIA GENERAL
DOC. Nº 41291/24
EXP. Nº 2830229

426

Que, el numeral 1.2.1 del artículo 1° del Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS, señala que los actos de administración interna de las entidades están destinados a organizar o hacer funcionar sus propias actividades o servicios. Estos actos son regulados por cada entidad, con sujeción a las disposiciones del Título Preliminar de esta Ley, y de aquellas normas que expresamente así lo establezcan;

Que, teniendo en cuenta que el Gobierno Electrónico es la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector público, con el objetivo de brindar mejores servicios al ciudadano e incrementar la eficiencia, la transparencia y la participación ciudadana;

Que, las facilidades para conectarse a las redes han aumentado; además, las aplicaciones y el software son cada vez más amigables y accesibles, de este modo todos tienden a conectarse en una red para compartir los recursos, pero esa facilidad de conexión también representa un aumento en los riesgos de que la información y los recursos de una organización puedan ser vulnerados;

Que, resulta necesario implementar medidas de seguridad para proteger la información y los activos de la Entidad. Seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; aunque no se puede alcanzar el 100% de seguridad, la tendencia debe ser llegar a ese valor extremo;

Que, los hackers, crackers están vigilando permanentemente las redes con el fin de encontrar las vulnerabilidades o debilidades de un sistema de información, el desarrollo del software ha permitido hacer cada vez más fácil la configuración y su utilización, Internet también permite la conectividad de todo tipo de usuario, de esta forma las amenazas a la seguridad de la Información están latentes y en cualquier momento un servidor o dispositivo de red puede ser atacado con fines negativos a la imagen de la Institución, a su funcionalidad y otros aspectos;

Que, la información constituye uno de los recursos principales de una organización; por lo tanto, se debe proteger, mediante un conjunto de actividades, controles y políticas de seguridad que se deben implementar en base a recursos humanos, hardware y software;

Que, la seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, proveedores, clientes, accionistas y del nivel de seguridad de los medios técnicos;

Que, el gran desarrollo de las tecnologías de las telecomunicaciones y de la informática en las últimas décadas ha permitido el crecimiento exponencial del servicio de Internet. Al presente todos pueden acceder a este servicio; la información ha sido globalizada;

Que, habiendo comenzado en los años 80 con algunos miles de usuarios hoy se benefician de este servicio miles de millones. Tanto es así que según las últimas estadísticas el número de direcciones IP actualmente en uso en Internet alcanza los 3/4 de la capacidad total que permite el rango de direcciones IPv4;

Que, hoy en día es mejor tener una página WEB que no tenerla. El servicio de Internet permite a las Empresas y a cualquier Institución realizar publicidad de sus productos y

servicios, simplificar las transacciones, ganar tiempo, ahorrar recursos y compartir y acceder a la información. El E-commerce y el E-business permiten conducir los negocios por Internet. Para una Organización tradicional esto significa ampliar la distribución de su catálogo de ofertas prácticamente sin fronteras, lo cual abre su mercado de una manera nunca imaginada con un costo muy bajo;

Que, una página WEB constituye una herramienta incansable y económica de publicidad y mercadeo. Las unidades de producción de las Entidades llevan a cabo acciones orientadas por los siguientes factores determinantes: Ventajas competitivas, innovación tecnológica y acceso a los mercados;

Que, las nuevas tendencias revelan un creciente consenso en torno al impacto que tiene la innovación tecnológica para el desarrollo económico y mejorar el nivel de vida de los ciudadanos. La innovación tecnológica, es el resultado de quienes la crean y difunden (Universidades y Centros de Enseñanza, Centros de investigación), quienes la incentivan (Sector gubernamental) y quienes la utilizan económicamente (las empresas);

Que, por tales razones, resulta necesario **APROBAR** el Manual de Seguridad de la Información diseñado por la Oficina de Desarrollo Institucional y Tecnologías de la Información ORDITI – 2020;

En uso de las atribuciones conferidas por la Constitución Política del Estado, Ley N° 27783 – Ley de Bases de la Descentralización, Ley Orgánica de los Gobiernos Regionales, modificado por la Ley N° 27902, Texto Único Ordenado de la Ley 27444 - Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS, y facultades conferidas por la Resolución Ejecutiva Regional N° 018-2020-GRJ/GR, de fecha 27 de enero del 2020, el Gerente General Regional;

SE RESUELVE:

ARTICULO PRIMERO: APROBAR, el **MANUAL DE SEGURIDAD DE LA INFORMACIÓN**, a efectos de dar cumplimiento a la preservación de la información clasificada de acuerdo al nivel de sensibilidad y los requerimientos legales de privacidad; de conformidad a los fundamentos expuestos.

ARTICULO SEGUNDO: NOTIFICAR, con las formalidades de ley a las instancias competentes del Gobierno Regional Junín, para los fines pertinentes.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

GOBIERNO REGIONAL JUNÍN

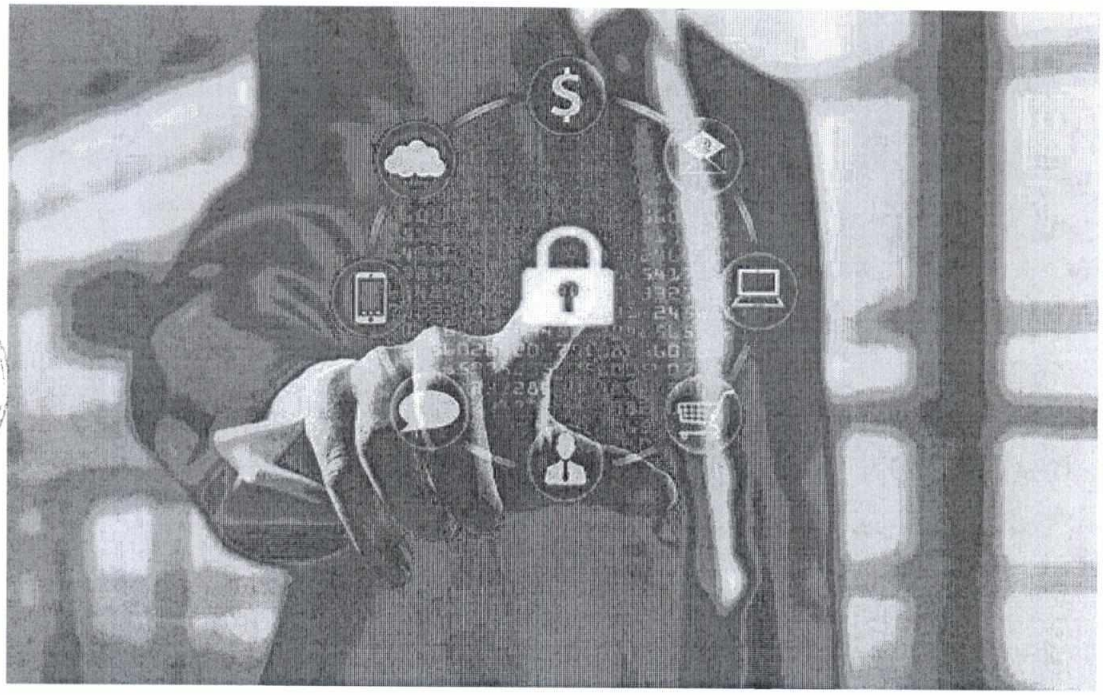
LIC. CLEVER RICARDO UNTIVEROS LAZO
GERENTE GENERAL REGIONAL

425

OFICINA DE DESARROLLO INSTITUCIONAL Y TECNOLOGÍA DE LA INFORMACIÓN ORDITI - 2020

REGIÓN JUNÍN

¡Trabajando con la fuerza del pueblo!



MANUAL DE SEGURIDAD DE LA INFORMACIÓN

18
418

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[1] de clasificar, proteger y autorizar el acceso a la información del **Gobierno Regional Junín** (GRJ), 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 Junín, 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 Junín.

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

CLASIFICACIÓN	NIVEL	DESCRIPCIÓN
Pública o no clasificada	**NCI0**	Información de uso interno y/o externo, con controles mínimos, cuya divulgación no tiene impacto sobre el Gobierno Regional Junín.
Interna	**NCI1**	Información con el propósito de distribución dentro del Gobierno Regional Junín, la fuga, divulgación de esta información podría causar un daño mínimo a la imagen y/o reputación del Gobierno Regional Junín 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 por los 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 autorizada de la información NCI2 podría dañar la imagen y/o reputación del Gobierno Regional Junín 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 Junín. La asignación de la clasificación de NCI3 debe ser autorizada por un directivo relevante en cada caso individualmente.

[1] Gerente, Sub Gerente o persona designada.

1.a 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 Junín.

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.b INFORMACIÓN DEL USO INTERNO (NCI1)

Información con el propósito de distribución dentro del Gobierno Regional Junín, la fuga, divulgación de esta información podría causar un daño mínimo a la imagen y/o reputación del Gobierno Regional Junín si fuera accedida por terceras partes.

La información NCI1 puede incluir lo siguiente:

- Informes
- Solicitudes
- Memorandos
- Resoluciones
- etc

1.c INFORMACIÓN DE DISTRIBUCIÓN CONFIDENCIAL (NIC2)

Información que está sujeta a acceso específicamente autorizado y su distribución es controlada, ya sea por personal por los 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 autorizada de la información NCI2 podría dañar la imagen y/o reputación del Gobierno Regional Junín 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.d 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 Junín. 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 Junín. 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 Junín 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 Junín deben utilizarse solamente para fines relacionados a las tareas y objetivos de cada oficina.
- Los recursos de propiedad del Gobierno Regional 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 Junín (correo electrónico, Internet, Intranet, SIAF, SIGA o cualquier otra contraseña de acceso) deben mantenerse en secreto y no deben proporcionarse a ninguna otra persona, sea o no trabajadores y funcionarios. El trabajador y/o funcionario debe procurar que nadie pueda utilizar los sistemas del Gobierno Regional Junín 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 usted 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 Junín en estricto cumplimiento de la legislación vigente sobre los derechos del autor y la ley de protección de datos personales.
- 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 Junín.
- El contenido de la información creados por los sistemas de información y comunicación y enviados por medio de recursos de propiedad del Gobierno Regional Junín, 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 Junín, al momento de la finalización del contrato de cualquier trabajador o funcionario. RRHH 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 vinculó 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 Junín para la distribución de información, archivos, publicación o ejecución de asuntos no relacionados del Gobierno Regional Junín, como por ejemplo material pornográfico y 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 el equipo software no autorizado o sin licencia, solo aquellos bajo licencia y autorizados por la Oficina de Desarrollo Institucional y Tecnología de la Información (ORDITI) del Gobierno Regional Junín.
- En caso de que sea necesario instalar algún "plugin" en el navegador (Internet Explorer), los colaboradores deberán verificar antes con ORDITI y Help Desk local si realmente es necesario utilizarlo.
- Siempre que exista una actualización de MS-Windows referida a problemas de seguridad, los colaboradores deben verificar con ORDITI y Help Desk la necesidad de realizar dicha actualización.
- La marca, el nombre y el logotipo de la empresa solo pueden utilizarse a los fines del trabajo y la prestación de servicios del Gobierno Regional Junín. Para utilizarlos con otros propósitos, es necesaria la autorización previa del ente perteneciente al Gobierno Regional Junín (Oficina de Comunicaciones).

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, tenga las siguientes precauciones:

- No discuta asuntos confidenciales o internos pendientes del Gobierno Regional Junín fuera de los lugares de trabajo o e presencia de terceros que no estén directamente involucrados con dichos asuntos.
- No discuta asuntos pertinentes del Gobierno Regional Junín con ninguna persona que no necesite tener conocimiento de esa información, tales como amigos, profesores, familiares, prensa, entre otros.
- No discuta asuntos pertinentes del Gobierno Regional Junín en áreas ajenas a la institución y, principalmente, en áreas y lugares públicos, tales como ascensores, aeropuertos, taxis, restaurantes, parques, bares y aviones.
- Adopte recaudos adicionales, en lo que respecta a la seguridad, al manejar información y documentos pertenecientes al Gobierno Regional Junín, en lugares públicos que presenten riesgos de exposición como los anteriormente citados.
- Solo utilice la información del Gobierno Regional Junín para fines profesionales o de trabajo.
- No facilite 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 suministre información de la institución a personas desconocidas o a quien no necesite conocerla y sin la respectiva autorización del responsable de la misma.
- Nunca suministre información de clientes o de proyectos a terceros que no estén formal o nominalmente vinculados a los proyectos y clientes en cuestión.
- Siempre adopte una actitud reservada con personas que intenten obtener información personal suya, de otros colaboradores o prestadores de servicios del Gobierno Regional Junín.
- Siempre solicite más de una identificación como garantía y comprobación de la identidad de su interlocutor cuando trate asuntos del GRJ, así como también algún dato de contacto, por ejemplo, teléfono y dirección debidamente comprobados.
- Relate inmediatamente a su superior cualquier incidente o sospecha de incidente de seguridad observado.
- No comparta 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 divulgue 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 Junín (y sus Sedes). La divulgación de información del Gobierno Regional Junín solamente debe efectuarse previa autorización por escrito y/o con motivo de exigencias legales o normativas.
- No utilice imágenes. Metodologías, procedimientos, presentaciones y otros documentos del Gobierno Regional Junín en presentaciones, libros, artículos, trabajos escolares o para cualquier otra finalidad sin el consentimiento expreso del responsable de dicha la información o será solicitada a través del portal de transparencia. En este supuesto, es obligatoria la mención del origen y la propiedad intelectual de la información que fue divulgada.

4. DOCUMENTOS

Considere como documento, a toda información puesta a disposición por medio de los recursos del Gobierno Regional Junín, 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 ORDITI Help Desk, 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, usted deberá cumplir las siguientes reglas:

- No deje 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.
- Mantenga todos los documentos y materiales de trabajo que contengan información del Gobierno Regional Junín en lugares adecuados para su almacenamiento y protegidos contra el acceso indebido, siguiendo las políticas de almacenamiento de datos establecidas por la ORDITI.
- No deje documentos clasificados como NIC2 o NIC3 con su contenido visible y a la mano de terceras personas.
- Guarde todos los documentos y la información en gavetas o armarios cerrados, y protéjalos su contenido de ser visualizado siempre que se aleje de su lugar de trabajo, independientemente del tiempo que estará alejado.
- No utilice recordatorios escritos (como contraseñas u otros accesos) que expongan información confidencial al ambiente externo (monitor, escritorio, etc).
- Organice 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 Junín[2] para el cierre de año para que sean almacenados en los archivos periféricos y posteriormente derivados al archivo central.

[2] DIRECTIVA GERENCIAL N° 008-2011-GR JUNIN-GGR/ORDITI

- 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 ejm. Vaciado de la papelera de reciclaje en MS-Windows o use las teclas "Shift + Supr")
- Verifique cuidadosamente a los destinatarios de la correspondencia para evitar errores en la entrega y, por consiguiente, el desvió de información, tanto por medio convencionales como electrónicos.
- Cuando envié información confidencial por el correo o mensajeros, utilice un protocolo de recepción que contenga los siguientes campos: nombre, documentos de identidad, cargo, departamento, fecha y horario de envió y de entrega.
- Utilice solo servicios seguros, aprobados y confiables por el Gobierno Regional Junín para el transporte de documentos.

5. ACCESO DE IDENTIFICACION DE PERSONAS

El acceso a las oficinas del Gobierno Regional Junín 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 Junín. En virtud de ello, deben seguirse las siguientes reglas:

- El personal de seguridad debe dar una identificación a cualquier persona
- Este siempre atento a cualquier persona extraña que circule en las oficinas del Gobierno Regional Junín.
- Comunique a la central de seguridad o al responsable local, 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 Junín 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 de recursos humanos y las cámaras de video vigilancia.
- Todas las personas naturales y jurídicas que estén visitando las oficinas del Gobierno Regional Junín deben portar su **tarjeta de acceso** (fotocheck) durante toda su permanecía 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:
    1. El personal o funcionarios deben de llevar la tarjeta de identificación personal en un lugar visible siempre.
    2. 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 funcionario.

3. En caso de pérdida o robo de la tarjeta de identificación, comunique el hecho inmediatamente al Departamento de Administración de Personal o a Recursos Humanos.
4. Las tarjetas de identificación de uso temporario deben ser devaluadas en la recepción del edificio cuando su portador deje las oficinas del Gobierno Regional Junín.
5. La tarjeta de acceso provisoria solamente podrá entregarse cuando el colaborador olvide la original, y deberá ser entregada con la autorización previa de un socio, director, gerente, supervisor o una secretaria del piso que lo conozca.

6. CORREO ELECTRONICO (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, cumpla 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 la cuenta, ejemplo: existente: mcarrion@regionjunin.gob.pe, el otro correo será: mcarrionp@regionjunin.gob.pe
- El tamaño de la cuenta es de 500MB, en caso de utilizar más recursos para almacenamiento debe comunicarse a la ORDITI para que se tome acciones e incrementar el tamaño de la cuenta.
- La comunicación por correo electrónico entre trabajadores y funcionarios es obligatoria, ORDITI se encargará de establecer la tecnología del correo electrónico, así como los backups respectivos. No utilice cuentas personales de correo electrónico para comunicarse o para transmitir cualquier otro tipo información de 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 transmita por correo electrónico a otras cuentas de correo electrónico fuera del ambiente de Gobierno Regional Junín, archivos anexados que contengan información clasificada como NIC2 o NIC3. En caso que sea necesario él envió electrónico de algún documento o archivo que contenga este tipo de información, usted debe obligatoriamente protegerlo para evitar la lectura indebida, utilizando una contraseña de la aplicación en que lo genero, como por ejemplo una contraseña de Winzip, Winrar, 7-Zip, Word, Excel etc, o alternativamente, algún recurso criptográfico disponible en la institución. Nunca envié en el mismo correo electrónico un mensaje protegido y las contraseñas o claves cristológicas utilizadas.
- No envié mensajes internos o externos que puedes perjudicar la imagen y/o reputación del Gobierno Regional Junín, tales como chistes, material de carácter sexual, imágenes videos (con extensiones .mpeg .avi u otras), música (con extensiones .mp3, .wav u otras), juegos, mensajes o textos de contenido étnico, criminal, religioso, político, o que pueda interpretarse como inofensivo.

- Cualquier correo identificado que haga envió de SPAM, primeramente, será amonestado formalmente, y de reiterarse será deshabilitado.
- No cree ni reenvié 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 a cliente o terceros. 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.
- Este 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.
- Tenga 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 Junín, sin previo aviso.
- Verifique 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 Junín, tienen un tamaño limitado, por lo tanto, verifique que la suya siempre se encuentre dentro de los límites establecidos, transfiriendo toda la información referida a trabajos a los respectivos archivos técnicos (FTP institucional, Dropbox, One Drive, Google Drive, etc.). En caso de que sea necesario que usted mantenga una copia temporaria de alguna información o correspondencia, la misma deberá ser transferida a su computadora.

7. TELEFONÍA

Los recursos de telefonía son puestos a disposición para tratar asuntos relacionados con los negocios de la institución y por concesión del Gobierno Regional Junín, 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.

- Tenga cuidado al dejar a una persona esperando en línea con el teléfono descolgado, permitiendo que oiga asuntos confidenciales del Gobierno Regional Junín. 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 Junín, 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 divulgue más información que su nombre y el nombre del Gobierno Regional Junín, excepto cuando total certeza de la identidad y las intenciones de su interlocutor.
- No discuta asuntos confidenciales con interlocutor desconocidos 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 Junín y si esto fuera indispensable, hágalo de forma discreta, asegurándose de la conversación no esté siendo oída por otras personas.

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 disquete 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 Junín sean perjudicados por un virus, usted debe cumplir las siguientes reglas:

- Mantenga siempre su antivirus actualizado (ESET endpoint antivirus).
- Si no tuviera instalado su antivirus exija a Help Desk que lo instalen.
- Programe su antivirus para realizar un scan en horas de almuerzo principalmente para que no interrumpa su trabajo una vez por semana, si tiene duda contacte con Help Desk.
- Realice un scan de su 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 Junín para actualizar el antivirus, Póngase en contacto con Help Desk 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 Help-Desk ORDITI.

- En caso de problemas con el software de antivirus, no desístale, inhabilite, ni intente reconfigurarlo. En estos casos contáctese inmediatamente con Help Desk ORDITI.
- Verifique el software y los archivos utilizados, o que serán utilizados en las computadoras y la red del Gobierno Regional Junín en relación con la existencia de virus siempre que:
    - ✓ Vaya enviarlo a otra apersona.
    - ✓ El software fue recientemente adquirido.
    - ✓ Que haya descargado archivos de internet o de otras fuentes.
    - ✓ 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 Junín.
- No instale ningún software que no esté autorizado y posea una licencia obtenida por Gobierno Regional Junín. En caso de que necesite instalar en navegador (Internet Explorer) algún complemento o "plugins", verifique antes con Help Desk si realmente es necesario utilizarlo y si la versión es la autorizada por el Gobierno Regional Junín. 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 Junín debe ser protegida en los medios de almacenamiento electrónico, tales como computadoras, de CD, DVD y USB.

Para ello siga 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, utilice algún tipo de encriptación y proteja con contraseña los archivos con información confidencial (Comprimido con winrar, contraseña a office, etc).
- No comparta archivos, directorios o unidades de disco en las notebooks y desktops.
- No permita que otras personas utilicen su computadora, sus conexiones de red, sus servicios de Internet y otros recursos.

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 usted.

Cumpla 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 las anote 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 temporaria 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 Junín, no utilice ninguna de las contraseñas que utiliza normalmente en los sistemas del Gobierno Regional Junín.
- 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 Junín, 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 HelpDesk-ORDITI de la veracidad de la solicitud antes de realizar los procedimientos de cambio.
- Cambie sus contraseñas dentro de un máximo de 90 (noventa) días, aún 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 HELP DESK-ORDITI 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 HELP DESK-ORDITI

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 GRJ, 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 Junín o fuera de las mismas.

- Si sale con el equipo para cualquier evento programado u otro, evite andar con el equipo del Gobierno Regional Junín por lugares peligrosos y sospechosos.
- Siempre mantenga sus datos en forma encriptada 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 HELP DESK-ORDITI.
- HELP DESK-ORDITI es el único personal 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 ORDITI 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 ORDITI se reserva el derecho de auditar periódicamente todos los equipos provistos por el Gobierno Regional Junín 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 HELP DESK-ORDITI para que solicite su aprobación.
- Antes de conectar equipos de un prestador de servicios en la red del Gobierno Regional Junín, el colaborador responsable por ese prestador de servicios debe contactarse con el personal de la ORDITI y solicitar su análisis y aprobación.

12. 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 Junín, en directorio públicos, incluso termporariamente, ya que cualquier persona autorizada o no, con acceso a la red de Gobierno Regional Junín podrá 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" de su equipo. En caso de tener dudas comunicarse con HELP DESK-ORDITI.
- 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 Junín.
- En caso de que sea necesaria la realización de backups especiales, además de los ya efectuados en forma periódica, comunicarse con HELP DESK-ORDITI.

15. 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 Junín. 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.

15.1 USO ADECUADO DEL INTERNET

Internet es un activo del Gobierno Regional Junín suministrado a los trabajadores y funcionarios para contribuir con los objetivos de la 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 del negocio. Toda información trasmitida por este medio será tratada como información relacionada con los objetivos de la institución, y debe estar alimentada a las normas enumeradas abajo. Las restricciones sobre uso NO-PRODUCTIVO sobre los usuarios serán aplicables por la ORDITI.

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 Junín.

- 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.
    - ✓ *Debe ser autorizada por su jefe inmediato*
    - ✓ *La autenticidad del software debe ser comprobada.*
    - ✓ *Han sido investigadas y determinadas las condiciones para su uso (incluyendo tarifas de shareware), y estas condiciones han sido cumplidas.*
    - ✓ *El software se instale de acuerdo a las políticas de seguridad mencionadas en este presente.*
    - ✓ *El software fue examinado por una versión actualizada del antivirus de la institución*
- Publicación de comentarios negativos, no profesionales del Gobierno Regional Junín 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 ORDITI 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 Junín.
- Una vez se detecte el uso indebido del Ancho de Banda por 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 RRHH para ser sancionado.

14. REDES SOCIALES

- Al usar el internet del GRJ 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 del GRJ o entes relacionados a este, siendo es ese caso será bloqueado el acceso al origen de dichos mensajes y reportado para su sanción respectiva a la oficina de RRHH.
- Prestar atención cuando publiquemos y subamos material con el uso del Internet del GRJ.
    - ✓ *Pensar muy bien qué imágenes, vídeos e información escogemos para publicar sin que afecte a la imagen del GRJ*
    - ✓ *No publicar nunca información privada que pueda perjudicar la imagen del GRJ*
- Escoger cuidadosamente a nuestros amigos.
    - ✓ *No aceptar solicitudes de amistad de personas que no conozcamos o perfiles falsos que puedan realizar ingeniería social.*
    - ✓ *Verificar todos nuestros contactos de forma permanente.*
- Proteger nuestro entorno de trabajo y no poner en peligro nuestra reputación y la del GRJ:
    - ✓ *Al registrarnos en una red social, usar nuestra dirección de correo personal (**no el correo de la empresa**)*

- ✓ *Tener cuidado de cómo representamos en Internet a nuestra empresa u organización*
- ✓ *No mezclar nuestros contactos de trabajo con nuestros amigos*
- ✓ *No guardar nuestras contraseñas de accesos a la red, sistemas, computadoras pertenecientes al GRJ en nuestro móvil*
- ✓ *Usar las funciones de seguridad de que disponga nuestro móvil para el uso de redes sociales con el internet del GRJ*

- Proteger nuestro teléfono móvil y la información guardada en él.
  - ✓ *Tener cuidado con lo que publicamos sobre otras personas, instituciones, empresas, organismos, etc con el internet del GRJ.*
- Informarnos del uso de las redes sociales.
  - ✓ *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.
  - ✓ *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 de nuestro teléfono móvil.
  - ✓ *Desactivar los servicios basados en la localización geográfica cuando no los estemos usando y/o usemos el internet del GRJ*

14. 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.

15. ¿CÓMO REPORTAR UN INCIDENTE DE SEGURIDAD?

Pueden reportar los incidentes de seguridad de la siguiente manera:

- Llamar a HELP DESK-ORDITI, teléfono: (+51064) – 602000 anexo 1504-1505.
- Enviar un correo a la siguiente dirección: incidentes@regionjunin.gob.pe.
- Contactar al responsable de Seguridad de IT.

16. SANCIONES

La violación de un control de seguridad o el incumplimiento del Manual de Seguridad de la Información del Gobierno Regional Junín, 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:

- Pérdida de acceso a determinados recursos, como por ejemplo correo electrónico, acceso a la red, acceso a los sistemas del Gobierno Regional Junín.
- Advertencia formal y escrita, dirigida por el representante del departamento de Recursos Humanos.
- Aplicación de sanciones laborales previstas en la legislación vigente de Perú.
- Proceso civil o penal dependiendo de la legislación vigente de Perú.
- Rescisión del contrato de prestación de servicios, cuando sea aplicable.