UNIVERSIDAD DE LA RIOJA

CIRCULAR 3/2020

EN DESARROLLO DE LAS INSTRUCCIONES PARA ADOPTAR CON CARÁCTER GENERAL EL RÉGIMEN NO PRESENCIAL PARA EL PERSONAL DE ADMINISTRACIÓN Y SERVICIOS DE LA UNIVERSIDAD DE LA RIOJA

20 de marzo de 2020

1.- DEDICACIÓN HORARIA.

En una situación de emergencia como en la que nos encontramos y en cumplimiento del deber de seguridad de las personas trabajadoras, se hace necesario promover y garantizar el trabajo seguro, de forma que la totalidad o una parte importante de la plantilla preste sus servicios desde su domicilio. Se minimiza así el riesgo de contagio y, en consecuencia, de contraer la enfermedad, al tiempo que se da continuidad a la actividad. No obstante, las medidas adoptadas para favorecer la modalidad de trabajo no presencial tienen un carácter excepcional y por tanto no podrán ser consideradas ni siquiera como modelo para el momento en el que la situación vuelva a la normalidad

De acuerdo con lo anterior, y con lo dispuesto en el artículo 88 de la Ley Orgánica 3/2018, de protección de datos y garantía de los derechos digitales, las personas empleadas públicas, tendrán derecho a la desconexión digital fuera del tiempo de su jornada habitual de trabajo, a fin de garantizar el respeto de los periodos de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

En consecuencia, los responsables de unidad deberán velar por que el trabajo desarrollado desde el domicilio, por las personas adscritas a sus unidades, no se extienda más allá de su horario habitual.

Salvo casos de urgente necesidad, no se deberán realizar llamadas a las extensiones de la Universidad de La Rioja, fijas o móviles, fuera del horario de 8:30 a 14:30 horas, de lunes a viernes. Fuera de la indicada franja horaria deberá utilizarse únicamente el correo electrónico.

Quedan excluidas de dicha restricción las extensiones fijas o móviles correspondientes a los responsables de unidad. No obstante, deberán respetarse, en la medida de lo posible, las franjas horarias y días indicados.

2.- RESOLUCIONES RECTORALES

Recuperada la normalidad, dentro de la situación excepcional, las unidades que deban extender resoluciones rectorales deberá solicitar número de resolución mediante correo electrónico a elisa.del-rio@unirioja.es y copia a pilar.armendariz@unirioja.es, indicando en el asunto "PETICIÓN NÚMERO DE RESOLUCIÓN". No deberán utilizarse las direcciones de las unidades (Secretaría General y Rectorado) para evitar la saturación de las mismas.

Una vez obtenido el número, las resoluciones deberán tramitarse a través de los canales y responsables ordinarios para su autorización, antes de ser enviadas para su firma, envío que se realizará del modo previsto en el párrafo anterior, indicando en el asunto “RESOLUCIÓN PARA FIRMA”.

3.- SEGURIDAD Y PROTECCIÓN DE DATOS

Es de obligado cumplimiento la observación de las normas y recomendaciones que desde la Vicegerencia de Gestión de la Información se dictan para el supuesto de realización de las actividades bajo la modalidad no presencial. Se acompañan a esta circular dichas normas y recomendaciones, estando a disposición de las trabajadoras y trabajadores en el enlace https://www.unirioja.es/servicios/si/seguridad/teletrabajo/

Date: 2020.03.20
14:42:35 +01'00'

Fdo.: Guillermo Bravo Menéndez-Rivas
GERENTE

UNIVERSIDAD DE LA RIOJA

Vicegerente de Gestión de la Información
Teléfono: 941 299 109
vice.gerenteginf@unirioja.es

SEGURIDAD EN EL TELETRABAJO

A continuación, se indican una serie de recomendaciones que pretenden minimizar los riesgos relacionados con la seguridad de la información en un escenario de teletrabajo, reduciendo los riesgos asociados a dicha actividad.

De forma general, se ruega que se sigan las instrucciones que la Universidad vaya facilitando para realizar las conexiones y accesos remotos a sus servicios.

Para incidentes o consultas en materia de seguridad de la información o aquellas que puedan afectar a la protección de datos de carácter personal, puede remitir su consulta o notificar el incidente al servicio de soporte por cualquiera de los canales oficiales:

1. Por la aplicación web: https://caur.unirioja.es
2. Por correo electrónico: soporte@unirioja.es
3. Por teléfono: 941 299 818

RECOMENDACIONES

- Al terminar de trabajar en algún servicio corporativo (webmail, aula virtual, escritorio remoto), recuerde finalizar la sesión o realizar la desconexión cuando deje de utilizarlo. Esto liberará recursos y evitará accesos no autorizados.
- Si instala certificados personales en equipos de utilización no habitual, proteja su uso con contraseñas y desinstálelo cuando ya no sea necesario.
- Evite transportar información corporativa en unidades extraíbles. Si fuera necesario, garantice que la información esté protegida de accesos no autorizados. No etiquete el dispositivo de forma que pueda reconocerse el contenido de este. Extreme las precauciones para evitar pérdidas u olvidos accidentales.
- Evite descargar información corporativa en dispositivos propios (teléfonos, equipos personales, etc.). Si fuera necesario, mantenga las medidas de seguridad para que no puedan acceder terceras personas, incluidas aquellas que puedan compartir el equipo.
- Evite imprimir o transportar información en soporte papel. Caso de realizarse, extreme las precauciones y asegúrese de que no se realizan accesos no autorizados.
- Salvo que sea absolutamente imprescindible, evite descargar información que contenga datos de carácter personal. Antes de realizar cualquier descarga de este tipo de información, reflexione sobre si es completamente necesario. Si así fuera, asegúrese que lo realiza con las medidas de seguridad necesarias (realice la descarga por canales de conexión segura, tome medidas para que no sea accedido por personas no autorizadas) y conserve los datos durante el tiempo estrictamente imprescindible.
- Elimine los datos o copias locales realizadas, incluso de forma automática, en cuanto dejen de ser necesarias. Para la información sensible o que contenga datos de carácter personal, asegúrese de realizar un borrado seguro que no permita la recuperación posterior. Para la información en soporte papel, elimínela con procedimiento de destrucción segura.
- En reuniones virtuales, revise bien quiénes están invitados (no tiene que haber personal desconocido o no invitados).
- Proteja la información manteniendo su pantalla de miradas indiscretas.

Vicegerente de Gestión de la Información
Teléfono: 941 299 109
vice.gerenteginf@unirioja.es

- Bloquee la sesión de trabajo cuando se ausente del equipo para evitar accesos no autorizados o acciones accidentales.
- En ningún caso guarde o cachee contraseñas cuando se pida una autenticación en un servicio web, como es el caso de Office365, Outlook accesible vía web, plataforma virtual de docencia, etc.
- Si se produce cualquier pérdida o sustracción de información corporativa, con especial atención a información sensible o que contenga datos de carácter personal, comuníquelo de inmediato al servicio de soporte por cualquiera de los canales oficiales.

Si estas medidas son importantes tenerlas siempre presentes, más primordiales son aún en un ambiente de teletrabajo, en el que el equipamiento puede ser compartido por más de una persona y puede estar más expuesto a las vulnerabilidades del exterior o a la instalación de aplicaciones de dudosa seguridad.

Tengamos en cuenta que en nuestras casas nos enfrentamos a un virus al que podemos contener aislándonos. En el caso de los virus informáticos todos seguimos conectados a través de la red de datos. **Si se infecta uno, nos infectamos todos**.

A continuación, se indican unos enlaces a unas recomendaciones relacionadas con la seguridad.

- Recomendación de ciberseguridad para usuarios del Centro Criptológico Nacional
- Recomendaciones ante ataques de "phishing" para personal en teletrabajo
- Recomendaciones frente al COVID-19 VIRTUAL

En el siguiente enlace encontraréis información más detallada relacionada con aspectos de la seguridad.

Por último, una recomendación que, sin tener que ver con la seguridad, es importante tenerla en cuenta en un entorno de teletrabajo. Se trata del uso de la red de datos, concretamente de su ancho de banda, que hoy en día cobra especial relevancia. El ancho de banda es un recurso limitado que compartimos entre todos y por eso, para evitar problemas de rendimiento, debemos usarlo con prudencia. Tenemos que limitar los servicios que más lo usan -como la videoconferencia- a los casos que realmente se necesiten; en el resto, la audioconferencia sin el video tendría que ser suficiente para nuestro quehacer diario.